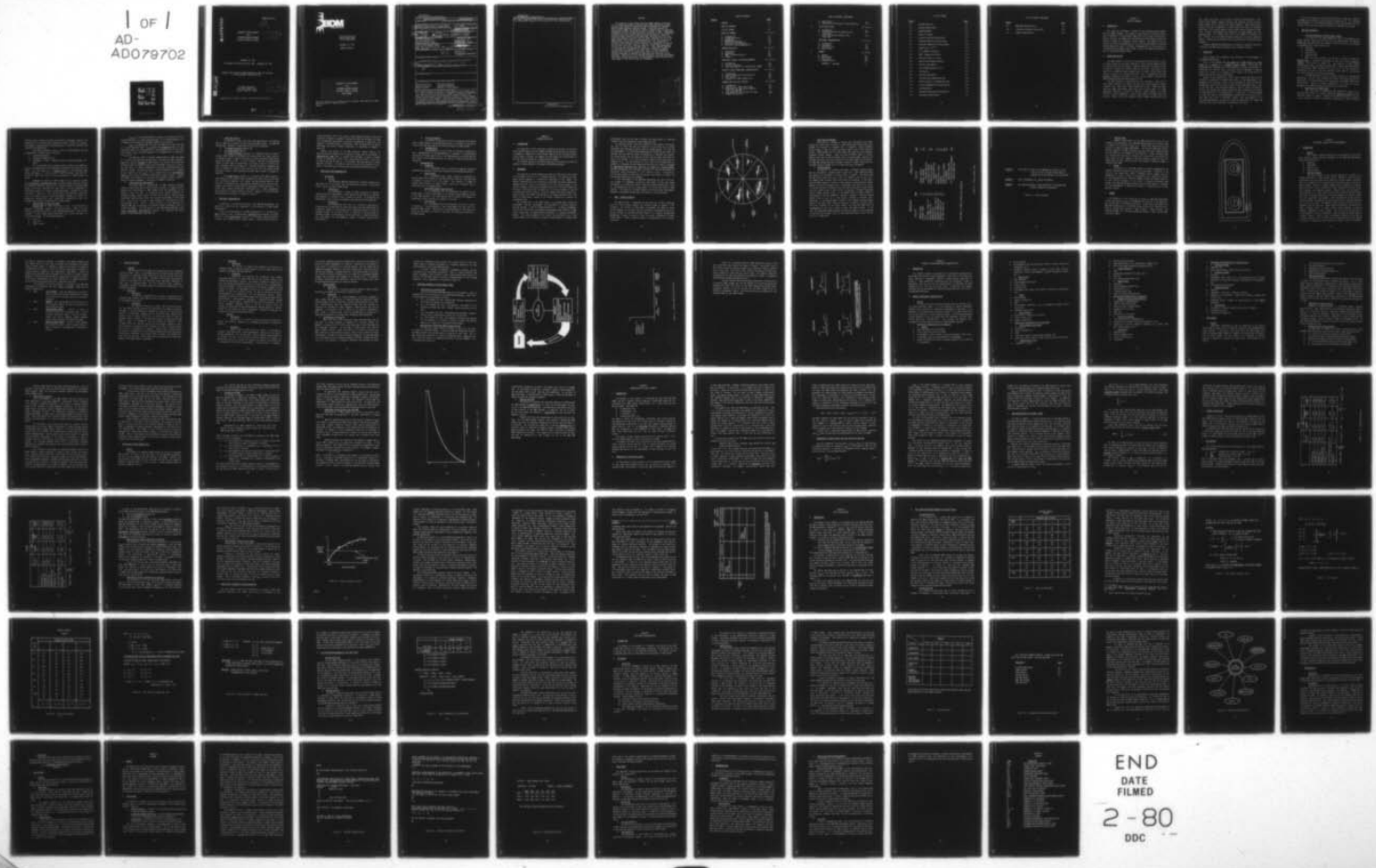
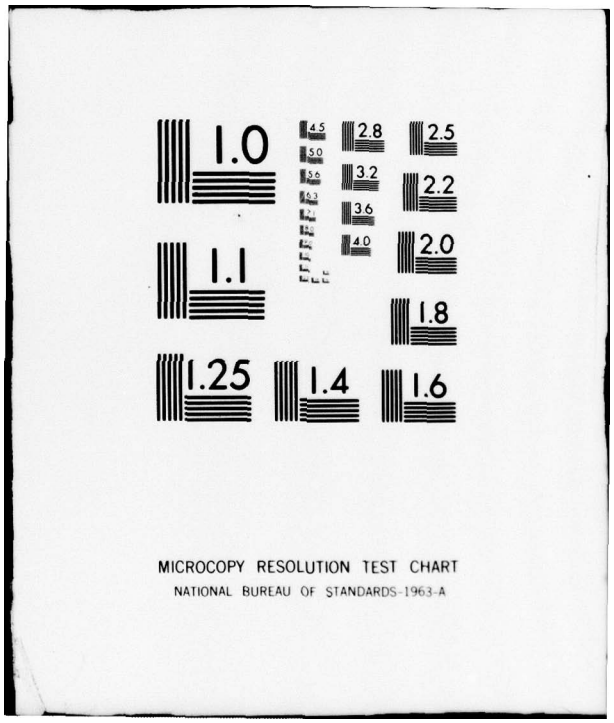
AD-A079 702 BDM CORP MCLEAN VA F/G 15/6
MEASURES OF EFFECTIVENESS FOR SHIPBOARD NUCLEAR WEAPONS PHYSICA--ETC(U)
DEC 79 W T OBER, C H HANKS, M F SHIELDS N60921-79-C-0101
UNCLASSIFIED BDM/W-79-729-TR NL

1 OF 1
AD-
AD079702



END
DATE FILMED
2-80
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
6.3
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

BDM/W-79-729-TR

MEASURES OF EFFECTIVENESS FOR SHIPBOARD NUCLEAR WEAPONS PHYSICAL SECURITY SYSTEMS

December 24, 1979

Final Report for Period June 25, 1979 - November 25, 1979

Prepared under Contract Number N60921-79-C-0101 for the Naval Surface Weapons Center/White Oak

The BDM Corporation
7915 Jones Branch Drive
McLean, Virginia 22102

7915 Jones Branch Drive
McLean, Virginia 22102
Phone (703) 821-5000

December 24, 1979

BDM/W-79-729-TR

MEASURES OF EFFECTIVENESS FOR SHIPBOARD NUCLEAR WEAPONS PHYSICAL SECURITY SYSTEMS FINAL REPORT

This work sponsored by the Naval Surface Weapons Center/White Oak under NAVSWC Contract No. N60921-79-C-0101.

4508A/79W

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER / 2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) (6) MEASURES OF EFFECTIVENESS FOR SHIPBOARD NUCLEAR WEAPONS PHYSICAL SECURITY SYSTEMS.	5. TYPE OF REPORT & PERIOD COVERED Final Report Jun. 25, 1979-Dec. 25, 1979
	6. PERFORMING ORG. REPORT NUMBER BDM/W-79-729-TR (14)
7. AUTHOR(s) (10) W. T. Ober II, J. C. Evans, C. H. Hanks, M. L. Fineberg, M. F. Shields, J. Schmaars	8. CONTRACT OR GRANT NUMBER(s) (15) N60921-79-C-0101
9. PERFORMING ORGANIZATION NAME AND ADDRESS The BDM Corporation 7915 Jones Branch Drive McLean, Virginia 22102	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 78012N; S0812-SL: S0812-SL-001; 9N78JH.
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Surface Weapons Center White Oak, Silver Spring, MD 20910 Attn: Code N44 (11)	12. REPORT DATE Dec [redacted] 79 (12) 92 (24)
	13. NUMBER OF PAGES 94
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)	15. SECURITY CLASS. (of this report) UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION UNLIMITED.

(9) Final rept. 25 Jun - 25 Dec 79,

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Physical Security	Statistical Analysis
Behavioral Science	Shipboard Operations
Nuclear Weapons	Measures of Effectiveness

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This report provides an analysis of the shipboard nuclear weapon physical security problem and develops a framework of measures of effectiveness (MOE) which can be used to objectively assess, evaluate, and compare the performance and effectiveness of physical security systems for shipboard nuclear weapons. Topics covered include: Identification of measurable security system operational characteristics; Definition of functional measures of effectiveness; Methods for determining (over)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

391 962

20. (Cont.) functional MOE values; and Integration of functional MOEs into combined MOE expressions for evaluation of total SNWS systems.

ABSTRACT

The shipboard nuclear weapon security (SNWS) problem is analyzed and a framework of measures of effectiveness (MOE) developed to assess, evaluate, and compare the performance and effectiveness of shipboard nuclear weapons physical security systems. Functional measures of effectiveness (FMOE) are defined in terms of probabilities for detection, assessment, reaction, and neutralization of threats to SNWS. Operational characteristic data for SNWS systems are identified in terms of measurable quantities which influence system functional performance. Means for evaluating FMOE probabilities are described, including use of the shipboard environmental simulation facility (SESF) scheduled for use in the SNWS Program. Three types of combined MOE for total ship security are defined as functions of the FMOE probabilities: the probability of security within shipboard zones of interest; the probability of security for the total ship; and a security index for a total SNWS system which reflects how well balanced an SNWS system is. These combined SNWS MOE are analyzed using non-parametric statistical techniques to address system evaluation problems at the fleet level. Linear programming techniques are applied to system design problems at the fleet level. Possible approaches to SNWS MOE for deterrence and recoverability are described. Application of the SNWS MOE methodology to system requirements definition, system formulations, and development of SNWS evaluation data requirements in the SNWS Program are recommended.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

LIST OF FIGURES

LIST OF FIGURES (CONTINUED)

CHAPTER 1
EXECUTIVE SUMMARY

A. INTRODUCTION

This study was performed in support of the Shipboard Nuclear Weapon Security (SNWS) Program. The purpose of the study was to develop a framework of measures of effectiveness (MOE) which can be used to objectively assess, evaluate, and compare the performance and effectiveness of physical security systems for shipboard nuclear weapons. The objective was to provide an evaluation methodology to aid in the accomplishment of the SNWS program objective, which is to make a recommendation for the selection of an engineering development model (EDM), based on the demonstrated performance of advanced development models.

B. PROBLEM DEFINITION

The SNWS problem is driven by fleet operational activities in which U.S. Naval forces are routinely required to carry nuclear weapons as part of their missions of sea control, strategic deterrence, and show of force in hostile or potentially hostile areas of the world. Any threat to the security of shipboard nuclear weapons poses a threat to the Fleet's capability to perform its assigned missions. This, in conjunction with the paramount importance of security for U.S. nuclear weapons, requires that SNWS be maintained at the highest possible level.

The SNWS problem is characterized by its diversity. There are at least twenty distinct ship types which may carry nuclear weapons, some as transport only, others with launch capability as well. These ship types span the range from attack cargo ships with civilian crews, to surface combatants carrying a variety of tactical nuclear weapons, to fleet ballistic missile submarines. Within these twenty ship types there are distinct classes for which shipboard nuclear weapon configurations may

vary, either with time, or as a result of physical considerations. Shipboard nuclear weapons comprise tactical and strategic nuclear missiles, nuclear bombs, and U.S. Marine Corps special weapons. These weapons may be stored or carried in magazines, in launch tubes below decks, in launchers above deck, or on aircraft weapon stations under certain operational conditions. Security requirements and procedures for these weapons vary with operating mode, i.e., whether ships are in port (CONUS or overseas) or at sea. Finally, for all of these situations there are a variety of potential threats, ranging from disaffected crew to professionally trained terrorist elements.

A general SNWS MOE methodology must be capable of assessing the effectiveness of candidate security systems in any of these situations.

C. ASSUMPTIONS

Three "ground rule" assumptions were observed in the development of the SNWS MOE methodology.

First, it was assumed that the purpose of an SNWS system is to deny access to or control of a shipboard nuclear weapon. Accordingly the methodology was developed to provide measures of system effectiveness in performing this function alone. Particular actions subsequent to gaining access to or control of a shipboard nuclear weapon, and system ability to defeat these actions, were not considered.

Second, it was assumed that, within reason, appropriate data could be obtained or generated to support application of the methodology. This assumption was justified in part by the consideration that the SNWS MOE methodology itself would serve as a guide to data requirements and in part by the fact that, since the SNWS program is likely to involve the development of new concepts and systems, particular data assumptions could induce an undesirable bias in the methodology. In particular, it was desired not to limit the scope of the methodology by considering only currently available SNWS data, which is extremely limited. Data requirements of the developed methodology, and means for obtaining these data, are summarized below and discussed in more detail in the body of the report.

The third assumption was that the objective of study was to develop assessment tools ad not to design security systems per se. This required the development of an unbiased methodology which would neither favor nor disfavor any one security system configuration or approach over another.

D. SNWS MOE METHODOLOGY

1. Functional Measures of Effectiveness (FMOE)

As a result of the study assumptions, and the requirements for a general approach imposed by the diversity of the SNWS problem, the SNWS MOE methodology was based upon four primary functions which must be performed by any SNWS system. These functions are:

- Detection,
- Assessment,
- Reaction, and
- Neutralization.

MOEs for these functions are defined in terms of conditional probabilities of successful performance in the four security zones of interest. These zones of interest are: ship exterior, on board, weapon control/access areas, and weapon storage areas. These functional measures of effectiveness (FMOE), denoted by P_D (Z), P_A (Z), P_R (Z), and P_N (Z), respectively, for each of the four functions in each zone "Z", are defined for a given ship type in a given operating mode.

The FMOE probabilities are the primary variables for the SNWS MOE methodology. As such, they represent the direct input data required for application of the methodology to the evaluation of candidate SNWS system effectiveness. Values for these probabilities will vary, of course, depending on the SNWS situation and threat under consideration.

2. Determination of FMOE Values

The first step in determining FMOE probability values for a candidate SNWS system is to define appropriate threshold criteria for the functional events in question. Keyed to requirements/constraints inherent in the situation to which the candidate system applies, these threshold

criteria serve to define the events of detection, assessment, reaction, and neutralization in precise terms (detection within x minutes or y meters, for example), thereby making the determination of functional probabilities relatively straightforward.

With these threshold criteria, values for FMOE probabilities may be obtained by a variety of means including:

- Test and Evaluation,
- Mathematical Modeling, and
- Assessment of Data in Ongoing Security System Development Programs.

It is anticipated that a primary source of data for the SNWS program will be generated at the Shipboard Environmental Simulation Facility (SESF). With the capability for repeated trials to test candidate SNWS system performance in a wide variety of SNWS situations, the SESF will provide an ideal test bed for direct determination of FMOE probability values.

Mathematical modeling of FMOE probabilities as functions of SNWS system operational characteristic data, validated through empirical testing and regression analysis, provides an alternative means of obtaining FMOE values. Operational characteristic data refers to directly measurable or quantifiable aspects of security system performance. Examples are listed in Chapter 4, Section B. Test and evaluation, manufacturers' specifications, and ongoing security system development programs are sources for operational characteristic data. Operational characteristic data also includes quantification of human factors in SNWS systems.

3. Combined MOE for Total Ship SNWS

Combined MOE for SNWS incorporate all four of the functions of detection, assessment, reaction, and neutralization. There are three different combined MOE defined in the SNWS MOE methodology. Each provides a measure of overall SNWS system effectiveness for a given ship type in a given operating mode. The three combined MOE are:

- $P_{sec}(Z)$,
- P_{SEC}, and
- Security Index.

P_{sec} (Z) is the combined MOE for security in a given zone "Z" for a given ship type in a given operating mode. It is defined (equation 5-1 in Chapter 5) as a function of the FMOE probabilities in zone "Z".

P_{SEC} is a combined MOE for total ship SNWS for a given ship type in a given operating mode. P_{SEC} denotes the probability that full and sufficient security is provided overall, taking security in all four zones into account. P_{SEC} is defined (equation 5-2 in Chapter 5) as a function of the P_{sec} (Z)'s.

The Security Index is another combined MOE for total ship SNWS for a given ship type and operating mode. The Security Index provides a measure of how well balanced an SNWS system is by taking into account the different levels of importance which may be attached to security in each of the four zones of interest, depending on ship type, operating mode, and, possibly, threat. The Security Index is defined (equation 5-3 in Chapter 5) as a function of the P_{sec}(Z)'s also, through the use of zone weighting factors which reflect the relative importance of zonal security. A systematic means for establishing reliable zone weighting factors, based on analysis of expert judgement, is described in Chapter 5, Section G.

4. Single Ship Type Applications

The three types of combined MOE for SNWS represent different figures of merit which may be used to assess, evaluate, or compare the performance and effectiveness of SNWS systems which are candidates for use aboard a given ship type. In conjunction with costing information on candidate systems, these figures of merit may be used to identify those systems which meet minimum overall ship security requirements for the least cost. They may also be used to rank systems on a cost-benefit or cost-effectiveness basis. Finally, inverse solutions of the equations for combined MOE may be obtained to establish system requirements prior to system development. This application of the SNWS MOE methodology to the system requirements specifications problem is an important and useful aspect of the methodology's applicability.

5. Fleet Applications

In addition to the single ship type applications, the combined MOE for SNWS may be applied to the fleet-wide SNWS problem. The SNWS MOE methodology, in general, is applicable to two distinct problems:

- The system evaluation problem, and
- The system design problem.

The system evaluation problem is to determine which of several possible SNWS systems or configurations would provide the "best" security if deployed across a range of ship types. Different operating modes may be taken into account as well. In this situation, matrices of combined MOE figures of merit may be constructed, one figure of merit for each (ship type, candidate security system) pair. Standard statistical techniques may then be applied to analyze these matrices and solve the stated system evaluation problem. These techniques are described in detail in Chapter 6, Section B.

The system design problem, is to identify those SNWS systems or configurations which maximize SNWS throughout the fleet, while at the same time satisfying budgetary and system availability/applicability constraints. Alternatively the system design problem may be to identify those systems which satisfy minimum security requirements and minimize costs. In either case, standard optimization techniques (e.g., linear programming) may be applied to identify optimal solutions. Examples of these techniques are described in more detail in Chapter 6, Section C.

E. ADDITIONAL CONSIDERATIONS

In addition to the measures provided in the SNWS MOE methodology, two additional criteria may be considered in the evaluation of SNWS system effectiveness.

First, the effectiveness of an SNWS system may lie in its ability to deter attacks, as well as defeat them. Deterrence may be defined as system ability to place psychological "barriers" or "distances" between potential intruders and shipboard nuclear weapon targets. Taking different possible

threat motivation levels into account, these deterrent effects involve the perceptions induced in potential intruders of both the existence of negative consequences and absence of positive consequences of their acts. An approach to quantification of deterrence, based on application of social psychology and market research techniques, is described in Chapter 7, Section B.

Second, the ability of an SNWS system to recover 100% of its security-providing capabilities following an attack may be considered. A Recoverability Index (RI) is defined and evaluated in terms of system ability to reconstitute itself within prescribed time limits. The RI for an SNWS system may be used as a "tie-breaker" MOE assuming that all other measures are equal. A system's RI would be particularly relevant in situations in which multiple or diversionary attacks were considered feasible.

F. CONCLUSIONS AND RECOMMENDATIONS

1. Conclusions

a. Utility

The developed SNWS MOE methodology is general enough to be applicable to all ship types, under any operational scenario, for any given threat, and for any type of SNWS system.

b. Practicality

The methodology is based on sound principles of security system operational requirements. Data required for calculation of performance measures is available from a variety of sources. In particular the methodology is well-suited to accommodate data obtained from the SNWS SESF.

c. Flexibility

The methodology lends itself to a variety of applications. Evaluations can be performed for cases that range from the effectiveness of a detection system in a restricted zone to the overall merit of a set of candidate systems for the entire fleet. In addition to the evaluation of candidate systems, the methodology can be exercised to establish performance requirements for developmental systems, including design-to-cost considerations.

d. Ancillary Benefits

In addition to providing a tool for evaluating the effectiveness of SNWS systems, the methodology provides a "road map" to the definition of test data requirements for future evaluations of SNWS systems.

e. Implementation

The methodology is well-suited to interactive computerization. Implementation of the methodology on a computer is straightforward and would facilitate application of the methodology by providing analysts with simple, quick-response options for security system optimization and evaluation.

2. Recommendations

a. Automation

It is recommended that an interactive computer program be developed for purposes of exercising and applying the SNWS MOE methodology.

b. Human Factors

It is recommended that further research be undertaken to analyze human factor aspects of the SNWS problem, along the lines described in Chapter 4, Section C.5 of the report. Such research is needed to improve quantification of human factors, which will inevitably play a significant role in any SNWS system.

c. System Requirements Specifications

It is recommended that the methodology be applied to the establishment of system requirements in the design and developmental stages of the SNWS program. Such applications would mitigate the tendency of technology to drive solutions in a program of this type.

d. Test Planning

It is recommended that the methodology be used as a source of guidance in the development of data requirements and test plans for candidate SNWS systems. Application of the methodology in this way would ensure the performance of uniform, consistent, and unbiased evaluations in the SNWS program.

CHAPTER 2
PROBLEM DEFINITION

A. INTRODUCTION

The objective of this study was to perform an analysis of the shipboard nuclear weapons security (SNWS) problem and derive from this analysis a framework of measures of effectiveness (MOE) which can be used to objectively assess, evaluate, and compare the performance and effectiveness of physical security systems for shipboard nuclear weapons.

This chapter describes the SNWS problem and the associated constraints imposed in the development of the general SNWS MOE methodology.

B. BACKGROUND

The security of nuclear weapons has been and continues to be an area of the highest priority in U.S. defense planning. The security of shipboard nuclear weapons is of particular importance in this regard. The special characteristics and constraints associated with Naval operations, combined with the crucial role played by U.S. Navy nuclear assets in the overall strategic and tactical deterrent posture of the United States and the Navy's recurring mission to establish U.S. military presence in hostile or potentially hostile areas of the world, demand that special measures be taken to ensure that SNWS is maintained at the highest possible level. Any threat to SNWS poses a threat to the Fleet's capability to perform its assigned missions.

The ultimate goal of the SNWS program is to upgrade SNWS through the development, testing, procurement, and deployment of improved physical security systems. A specific program objective is ..."to make a recommendation for the selection of an engineering development model (EDM) of an SNWS system based upon the demonstrated performance of advanced development models." The study presented in this report was performed to aid in the accomplishment of this objective through the development of a general MOE

methodology which can be used to assess the effectiveness of candidate systems in providing shipboard nuclear weapon security.

Two important ground rules were observed in the conduct of the study. The first of these was that the objective of the study was to develop assessment tools and not to design security systems per se. This required the development of an unbiased methodology which would neither favor nor disfavor any one security system configuration or approach over another. The second ground rule was based on the fact that to assess the effectiveness of any system, it is first necessary to specify what that system is supposed to do. For the purposes of this study it was assumed that the purpose of a shipboard nuclear weapon physical security system is to assure no unauthorized personnel gain access to or control of a nuclear weapon. The MOE methodology was developed, therefore, to provide the means for evaluating system performance of this function alone. In particular, distinctions between various possible actions (once access or control has been accomplished) were not considered.

A final requirement of the SNWS MOE methodology was that it be flexible enough to accommodate evaluations that range in scope from system performance on a single ship type to fleet-wide system effectiveness. That is, the methodology had to be applicable to a diversified array of SNWS problems. The nature of the SNWS problem and the associated requirements imposed on the SNWS MOE methodology are discussed in the next section.

C. SNWS: PROBLEM DIVERSITY

The SNWS problem is compounded by the diversity of Naval platforms which can carry nuclear weapons, the different types of weapons in the inventory, the variety of operational environments and modes in which nuclear weapons are involved, and the different zones aboard ships which may be included in the SNWS envelope (Figure 2-1). Because the SNWS MOE methodology is meant to serve as a tool for overall assessment of system effectiveness, it must be general enough to be applicable in all of these situations.

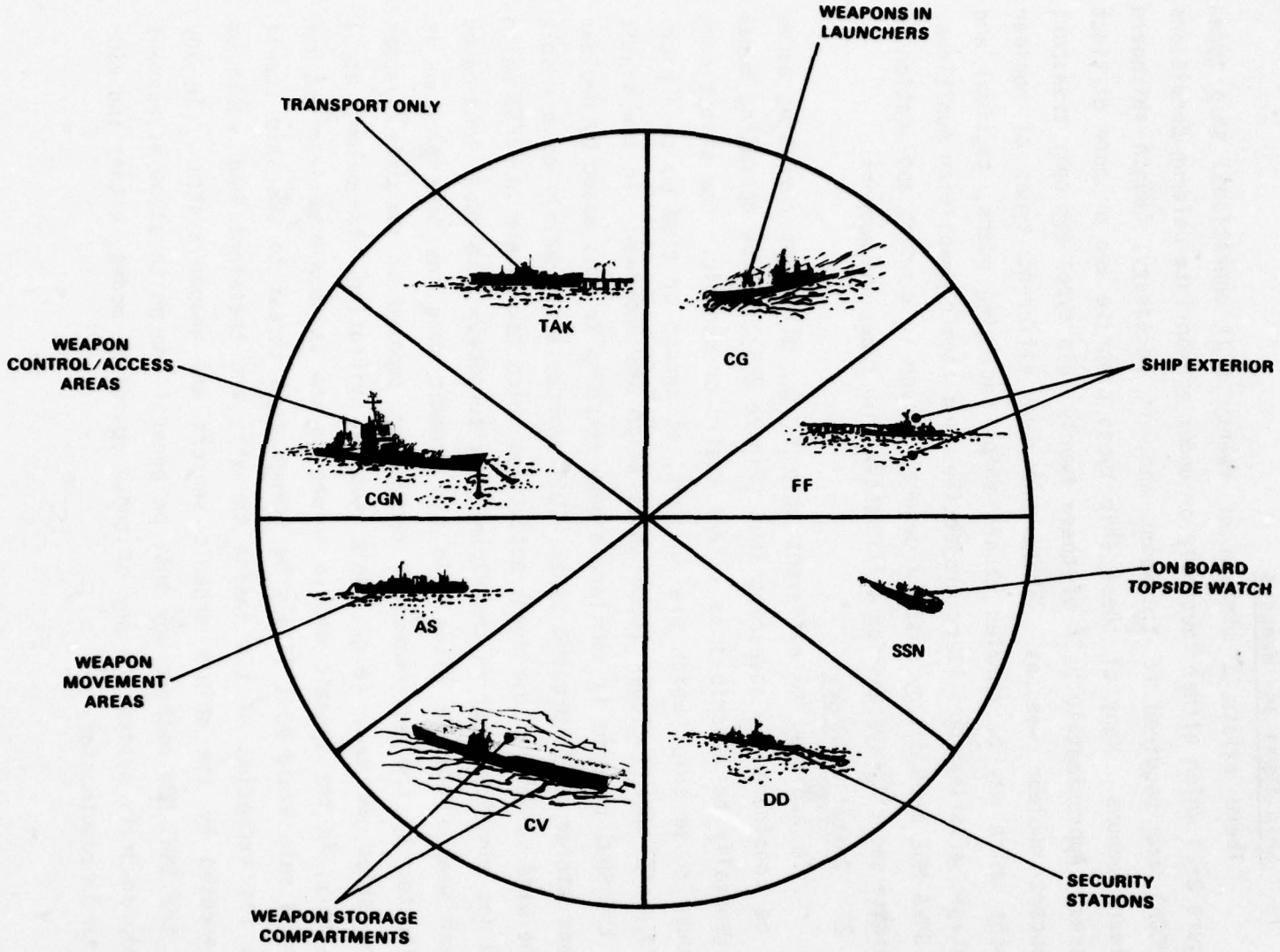


Figure 2-1. Problem Diversity

4508/79W

1. Ship Types and Weapons

There exists a minimum of twenty (20) operational ship types (Figure 2-2) which either routinely or under appropriate Defense Conditions (DEFCON) are required to transport and, if necessary, launch shipboard nuclear weapons. Many of these ship types comprise two or more distinct classes. Approximately half of these twenty ship types can only transport shipboard nuclear weapons. There are many different types of nuclear weapons which may be carried aboard ships including bombs, tactical and strategic missiles, artillery projectiles and atomic demolition munitions. The SNWS MOE methodology must be general enough to support application to candidate security systems for all of these ship types and weapons.

2. Operating Modes

In addition to different ship types, different operating modes must be considered in assessing SNWS (Figure 2-3). These operating modes may generally be described as either static or dynamic. The static mode includes those ships which are in port, at anchor or tied up to a pier. The dynamic mode includes those ships which are underway. In the static mode the SNWS problem is similar in many respects to that posed by nuclear weapons stored at land-based sites. Differences arise mainly as a result of the wide variety of different activities which take place in ports which would not normally occur in the vicinity of purposely "isolated" land-based nuclear weapon storage sites. In the dynamic mode the SNWS problem is complicated by the environmental conditions imposed on security systems aboard ships at sea, (e.g., ship motion, vibration, corrosion, etc.) Conversely, in the dynamic mode a threat to the shipboard nuclear weapons aboard a ship would most likely be viewed as a threat to the ship itself (with the exception of the inside threat), and therefore SNWS would be complemented by the ship's organic sensors and weapon systems. In any case, the SNWS MOE methodology must be general enough to allow assessment of ship security systems in any of these operating modes, either individually or in combination.

TRANSPORT ONLY		LAUNCH & TRANSPORT	
SHIP TYPE	ABBR	SHIP TYPE	ABBR
SUBMARINE TENDER	AS	AIRCRAFT CARRIER*	CV
DESTROYER TENDER	AD	AIRCRAFT CARRIER* (NUCLEAR PROPULSION)	CVN
OILER	AO	GUIDED MISSILE CRUISER	CG
FAST COMBAT SUPPORT SHIP	AOE	GUIDED MISSILE CRUISER (NUCLEAR PROPULSION)	CGN
REPLENISHMENT OILER	AOR	FAST FRIGATE	FF
AMMUNITION SHIP	AE	GUIDED MISSILE FRIGATE	FFG
AMPHIBIOUS ASSAULT SHIP(GP)	LHA	DESTROYER	DD
AMPHIBIOUS TRANSPORT DOCK	LPD	GUIDED MISSILE DESTROYER	DDG
AMPHIBIOUS ASSAULT SHIP	LPH	ATTACK SUBMARINE (NUCLEAR PROPULSION)	SSN
MSC ATTACK CARGO SHIP	TAK	FLEET BALLISTIC MISSILE SUBMARINE (NUCLEAR PROPULSION)	SSBN

*CAN LAUNCH IF ORGANIC AIRCRAFT ARE CONSIDERED

Figure 2-2. Nuclear Capable Ships

DOCKSIDE - SHIP TIED UP TO PIER, OR TO ANOTHER SHIP, WHICH IS ITSELF TIED UP TO PIER; COULD BE EITHER CONUS OR OVERSEAS IN ALLIED, NEUTRAL, OR CIVILIAN PORT

ANCHORED - SHIP AT ANCHORAGE SITE; CONUS OR OVERSEAS

UNDERWAY - SHIP UNDER OWN POWER; EITHER TERRITORIAL OR INTERNATIONAL WATERS, SURFACED OR SUBSURFACED

Figure 2-3. Operating Modes

3. Security Zones

Another unique aspect of the SNWS problem which must be considered in the formulation of an SNWS MOE methodology has to do with "zones of interest" for security (Figure 2-4). These zones range from the ship exterior to weapon storage compartments. The relative importance of maintaining security in these zones may vary with ship type, operating mode, and the nature of the weapons to be protected. In many instances there will be more than one zone of interest for a given ship, and security in these areas will be a subset of the total security system for the ship. These zones are also consistent with the concept of defense-in-depth in connection with SNWS.

4. Threat

The diversity of the SNWS problem is further compounded by the variety of potential threats which must be considered. In addition to the terrorist and paramilitary threat, shipboard nuclear weapons are also susceptible to hostile actions by disaffected crew, potentially harmful civilian demonstrations or intrusion attempts, enemy intelligence activity, or even criminal elements. To be useful in assessing candidate SNWS systems, the SNWS MOE methodology must be sufficiently general in approach to allow measurement of system effectiveness in countering any of these potential threats.

D. SUMMARY

The objective of this study was to devise an SNWS MOE methodology flexible and general enough to accommodate the diversity of the SNWS problem as described in the preceding sections. To meet these requirements the SNWS MOE methodology was formulated around certain basic functions which security systems must perform in any situation. These functions, and quantitative MOEs for evaluating system performance of them, are described in the next chapter.

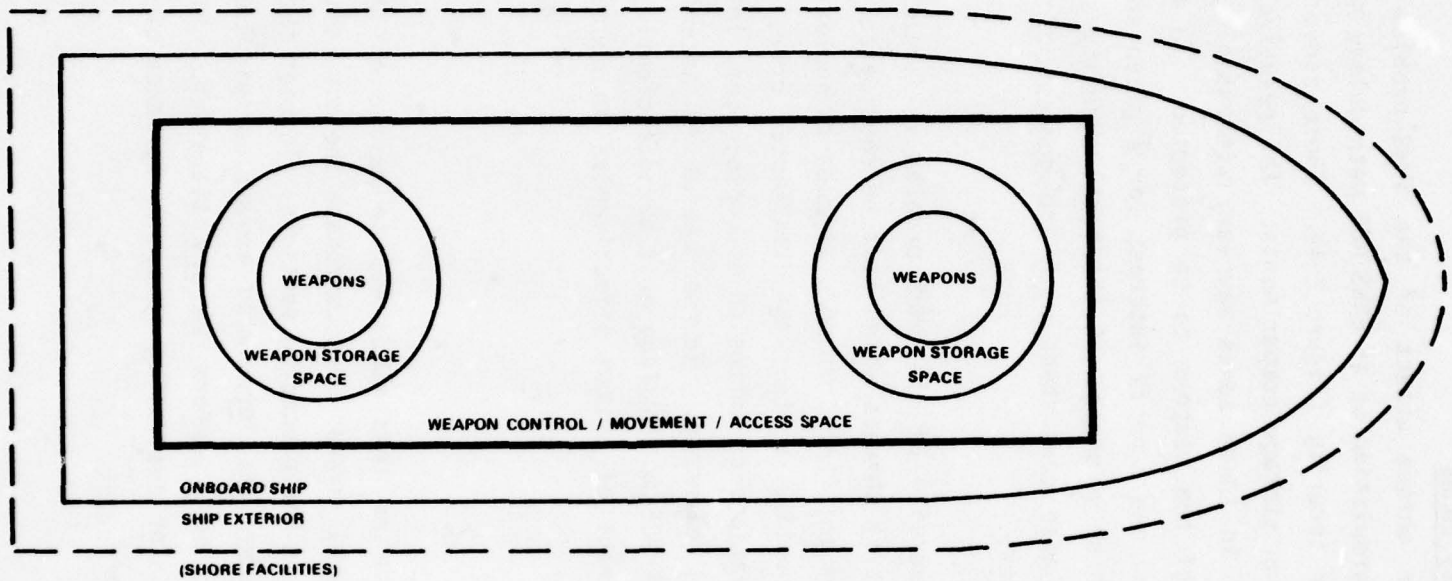


Figure 2-4. Zones of Interest

4508/79W

CHAPTER 3
FUNCTIONAL SECURITY SYSTEM REQUIREMENTS

A. INTRODUCTION

1. General

This chapter provides definition and description of the four basic security system functions considered in the SNWS MOE methodology. These four functions are:

- Detection,
- Assessment,
- Reaction, and
- Neutralization.

2. Security-in-Depth

The basic purpose of any security operation or system is to provide protection of some valuable asset. Because of their political significance and vast destructive capability, nuclear weapons have been, and in all probability will continue to be, protected using a security-in-depth concept. Security of weapons depends upon a combination of guards, physical barriers, secure storage facilities, communication checks, detection systems, and response systems. Aboard ships the existence of restricted areas, or zones, improves security by providing defense-in-depth and tends to increase efficiency by providing degrees of security compatible with operational requirements. These restricted areas may also provide for economy of operation by reducing the need for stringent measures for the ship as a whole. The degree of security required within a zone is dependent upon the type ship, weapon system configuration, and operational mode. Different areas, or zones, involve varying degrees of security interest, depending on their purpose. The entire ship may not have a uniform degree of security importance. Once the zones are established for a certain type or class of ship, a systematic approach can be used to provide an effective and efficient basis for measuring the various degrees of security in reference to the restriction of access, control of movement,

and type of protection required. For example, the weapons magazine and work spaces serve as inner rings of defense, and the general ship spaces serve as buffer zones. An increase in security may result in a reduction in operational efficiency. The use of security zones makes it possible to provide security compatible with operational requirements. Instead of establishing stringent security measures for the ship as a whole, varying degrees of security can be provided as required and as conditions warrant. In this way, interference with overall operations is reduced and operational efficiency can be maintained at a relatively high level.

The principle of security-in-depth is reflected in the SNWS MOE methodology by considering four basic zones of interest. These security zones of interest are:

- Zone 1 - SHIP EXTERIOR - That area beginning at the ship's brow, in the direction away from the ship; limited to the confines of the port facility in the dockside mode.
- Zone 2 - ONBOARD - That area bounded by the ship's brow, in the direction towards the ship, and ending with the topside deck watch.
- Zone 3 - WEAPON CONTROL AREA(s) - Area(s) in which an interface exists with the weapon itself. Zone 3 includes annunciator panels, security stations, command and control elements, weapon movement areas, tracking systems, and launching systems.
- Zone 4 - WEAPONS STORAGE AREA(s) - Area(s) in which weapons are located or stored. Zone 4 includes the entire gamut of locations, from magazines to launchers to aircraft.

B. SECURITY FUNCTIONS

1. General

SNWS MOE must provide a means for evaluating the total integrated security system. That is, the methdology must include the derivation and description of quantitative MOE which can be used to evaluate the effectiveness of a total SNWS system. Therefore, a functional classification scheme was developed with the functional areas applicable regardless of ship class or operating mode. The four functional areas: detection, assessment, reaction, and neutralization are defined and described in the following paragraphs.

2. Detection

a. Definition

The ability to become aware of an attack or penetration of a protected area, whatever the purpose of such an attack or penetration might be, and whatever the source.

b. Discussion

The detection function, by itself, does not provide security, but rather provides warning or an indication of a threat to security. The means or devices employed to perform this function will have varying degrees of proficiency, ranging from an indication that something has occurred with no further definition, to precise definition of what has happened. Other variables in the detection function include type coverage (point, linear, or volumetric) and the distance of detection. Also included within this function would be an intelligence network or capability insofar as it might provide information on plans or operations which could lead to a degradation of security. Access control systems perform the function of detection by discriminating between authorized and unauthorized entry of personnel into secured areas or spaces. Once detection of some form has occurred, results must then be transmitted to some other segment of the SNWS system for assessment.

3. Assessment

a. Definition

The ability to receive and determine the nature of a detected threat to security, analyze courses of action, make a decision for response, and communicate that decision.

b. Discussion

Processing and reporting the information from elements performing detection is a significant part of any security system in performing the assessment function. For example, electronic supervision of the lines connecting detection sensors to a control unit, or annunciators, must be considered in light of the ability of the threat to tamper with and defeat the system. The assessment function can be considered the "nerve center" of the total security system. It may be carried out manually, semi-automatically, automatically, or some combination thereof. Manual assessment is basically the human element with the attendant human factors considerations. Semi-automatic assessment is "machine-assisted" through the use of display panels, computer-assisted decision processes, and so forth. Automatic assessment occurs in the use of devices which are intruder activated and provide pre-determined response decisions. Consideration of the functional area of assessment is especially important for purposes of evaluating system effectiveness.

4. Reaction

a. Definition

The ability of a security system to provide an appropriate, timely, and effective response to an attempted penetration or threat to security.

b. Discussion

Reaction may be either active or passive. Such things as bulkheads, watertight doors, locked compartments, fences etc., are passive reaction mechanisms. For the most part, passive reaction imposes delay on an intruder and time for the active reaction elements to respond. An appropriate reaction is one which is suited to the nature of the threat and in conformance with security requirements. Too much force, or response,

could hinder shipboard operational capabilities, while too little might not be able to prevent degradation of security. Timeliness of the reaction is a key factor in evaluation of a security system. This can range from an immediate automated reaction to the time required for a reaction force to receive and implement a response decision. The effectiveness of the reaction function involves variables such as reliability in automated response systems and proficiency and armament of a reaction force. In addition, procedural requirements and limitations, such as use of deadly force, must be considered when evaluating the reaction function.

5. Neutralization

a. Definition

The ability of a security system to defeat or repel a threat and return all elements of the security system to normal.

b. Discussion

Any system, or system component, explicitly designed to repel, defeat, destroy, capture, or otherwise thwart an attacking or penetrating element could be classified as having neutralization as its function. Neutralization does not necessarily mean that the attackers or intruders are overcome by lethal measures. Neutralization can also be temporary, or reversible, such as repelling the attack or penetration. Other forms of neutralization could be accomplished by detaining or capturing the attackers or by disabling or damaging threat mechanisms.

6. Relationship of Functions

More than one of the functional areas described above may be applicable to a given element or component of a security system. For example, a Closed Circuit TV (CCTV) could contribute to both the detection and assessment functions. An individual on deck watch could visually detect unusual activity, assess the activity as a threat to security and make a decision to take preventive action, react to the situation by ordering potential intruders to halt and identify themselves or take them under fire, and neutralize the intruders through his actions, thereby contributing to all four functions. In general, therefore, the evaluation of total

security for shipboard nuclear weapons will require that all four functional areas be examined throughout all shipboard operations, for each class/type ship, and in each operating mode.

The four functions of detection, assessment, reaction, and neutralization are considered conditional. That is, these functions take place in sequence, and a failure in any of the functions would result in a failure for the total security system in accomplishment of its ultimate objective. This is graphically illustrated in Figure 3-1.

C. FUNCTIONAL MEASURES OF EFFECTIVENESS (FMOE)

1. Definition of Functional MOE

The four functions described above can be expressed in terms of probabilities to form the basis for the SNWS MOE methodology. These conditional probabilities are defined as follows:

- P_D = the probability that unauthorized personnel approaching a given security boundary will be detected
- P_A = the probability that, once detected, the threat will be properly evaluated and that a proper reaction decision will be made
- P_R = the probability that, once detected and assessed, an appropriate, timely, and effective reaction will be provided
- P_N = the probability that, once detected, assessed, and reacted to, the response is sufficient to prevent a threat from gaining access to, or control of, a shipboard nuclear weapon.

2. Application of Functional MOE to Security Zones

As previously stated, security-in-depth is implicit in the zones of interest in the SNWS problem. To make the SNWS MOE methdology flexible, the FMOE probabilities defined above are applied to each zone. This is done because all functions of a security system may apply in each security zone, from ship exterior to immediate proximity of nuclear weapons. This is represented in Figure 3-2.

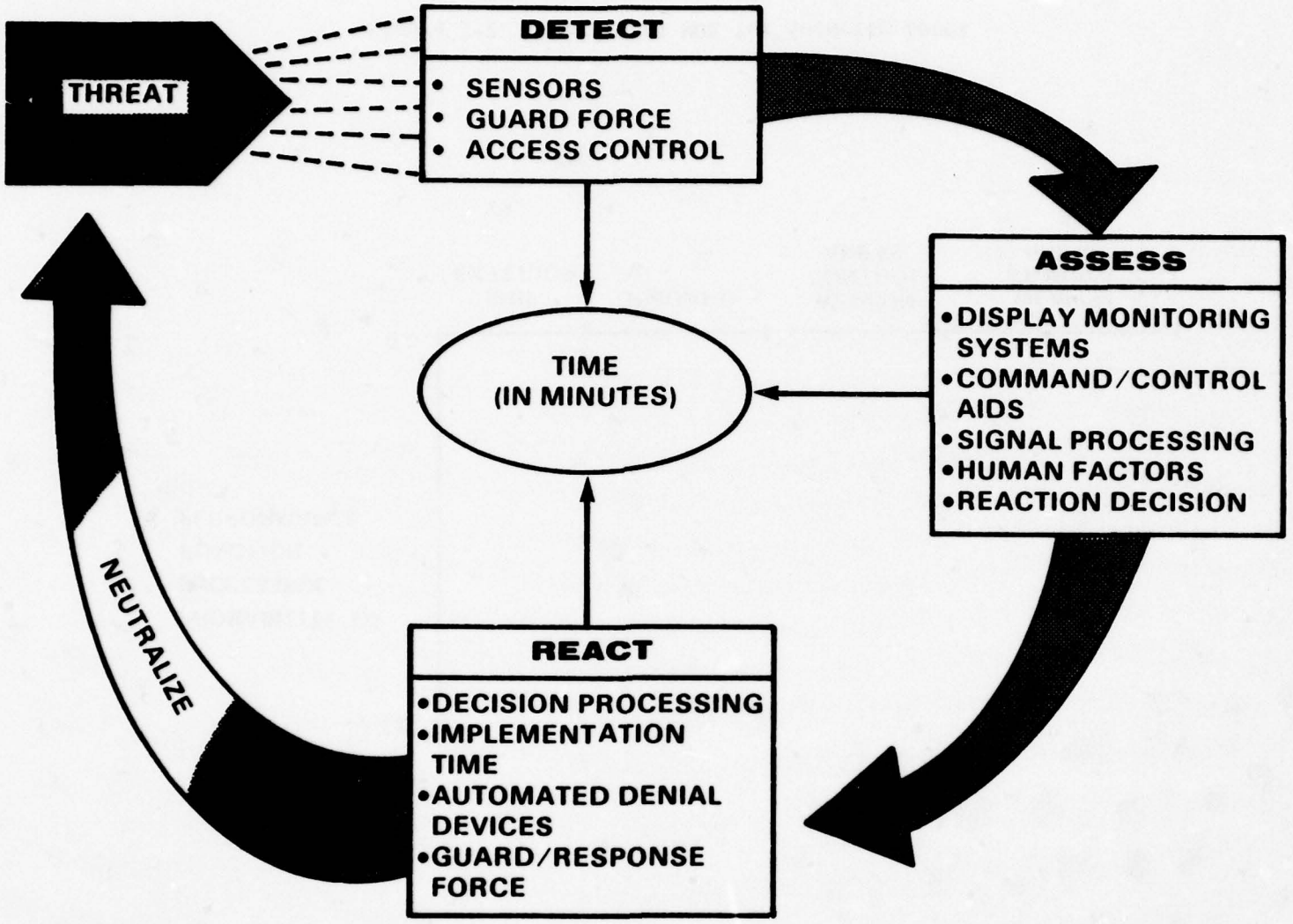


Figure 3-1. Security Function Relationships

4508/79W

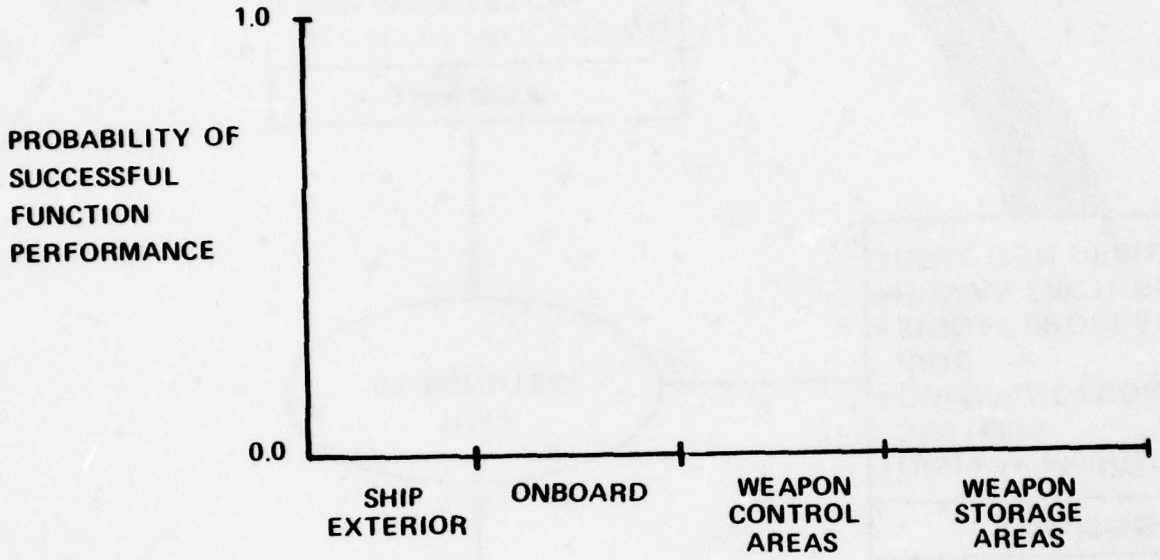
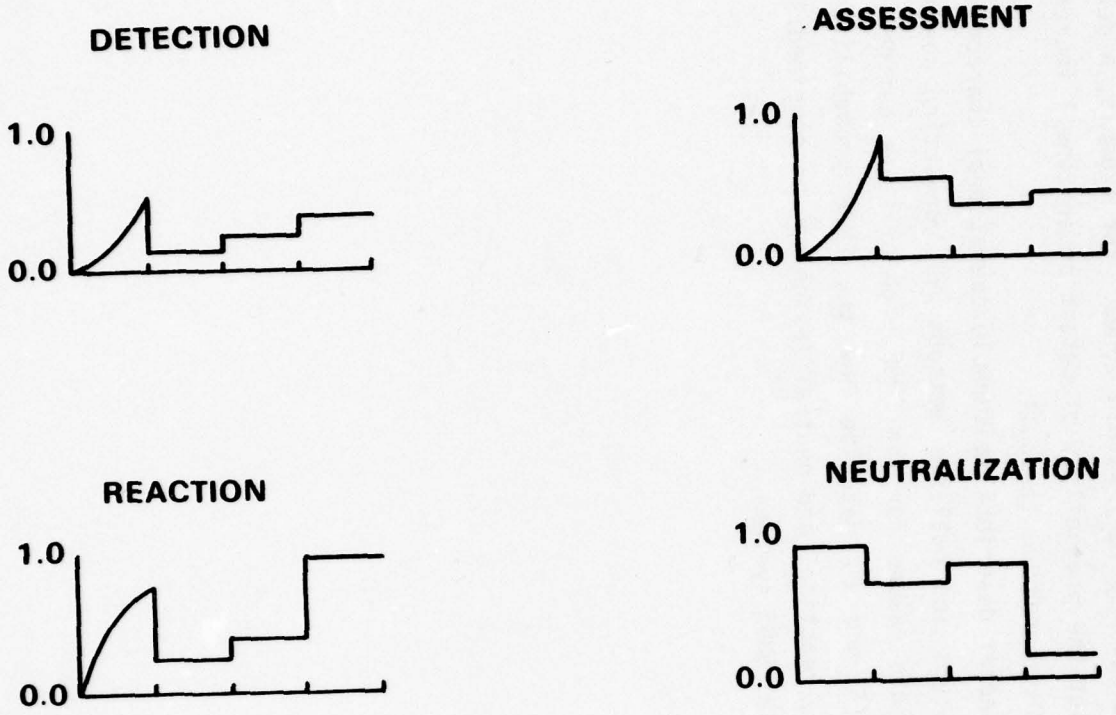


Figure 3-2. Functional MOE for Security Zones

Figure 3-3 illustrates possible FMOE probability values in the four functional areas across the zones of interest. Horizontal lines in the figure indicate a constant probability of successful function performance in that zone. The curving lines indicate the possibility that functional probability values may vary within zones. For example, a detection system may be such that the probability of detection in zone 1 increases as the penetrating element approaches the hull.

The next chapter describes measurable operational characteristics of possible SNWS systems and outlines methods for converting operational characteristic data into values for the FMOE probabilities defined above. Succeeding chapters (5 and 6) describe how the FMOE probabilities for detection, assessment, reaction, and neutralization may be combined to form integrated MOE for total SNWS systems.



OVERALL SYSTEM INVOLVES ALL FOUR FUNCTIONS. SYSTEM COMPONENTS, HOWEVER, MAY ONLY MAKE SENSE IN ONE OR TWO FUNCTIONAL AREAS.

Figure 3-3. Functional Measures of Effectiveness

CHAPTER 4
SECURITY SYSTEM OPERATIONAL CHARACTERISTICS

A. INTRODUCTION

This chapter provides a description of operational characteristics associated with security system components within each of the functional areas (Detection, Assessment, Reaction, Neutralization) described in Chapter 3. These operational characteristics are expressed in terms of measurables that can be used for quantification to determine the FMOE probabilities for the four functional areas. In addition, this chapter describes sources and methods for obtaining quantified data to be used in the SNWS MOE methodology.

B. GENERAL OPERATIONAL CHARACTERISTICS

1. General

In order to provide the requisite data input for the four security system functional areas, it is first necessary to identify measurable elements which contribute to functional performance in each area. It is important to note that these functional elements will be quantified either by test and evaluation or other analytical means. The following paragraphs provide examples of security system functional components and their associated operational characteristics. The listings are examples only. Adjustments are anticipated as the overall SNWS program progresses.

2. Operational Characteristics of Detection

a. Sensors

- Mean time between failures (MTBF),
- False alarm rate/reliability (FAR),
- Environmental levels (refers to the environmnetal limits which, if exceeded, cause sensor performance to be degraded),
- Defeat vulnerability (refers to system susceptibility to spoofing or disablement),

- Area coverage,
- Discernability and discrimination (refers to sensor sensitivity thresholds), and
- Phenomena coverage (motion, vibration, noise, heat, pressure, electrical, visual, electromagnetic, pattern recognition, stress, etc.).

b. Guard Forces

- Zone coverage,
- Area coverage within zones,
- Visual acuity,
- Vigilance, and
- Performance aids (night vision devices, binoculars, annunciators, etc.).

c. Lights

- Area coverage,
- Defeat vulnerability,
- MTBF,
- Environmental conditions (e.g., % background average reflectance), and
- Redundant power source.

d. Access Control

- Reliability of identity verification,
- Rate of access, and
- Defeat vulnerability.

3. Operational Characteristics of Assessment

a. Display Monitoring Systems

- Reliability,
- Defeat vulnerability,
- MTBF,
- Type signal (audio, visual)/signal strength, and
- Resolution levels (refers to level and type of detail displayed).

b. Command/Control Aids

- Automated vs. manual,

- Decision processing time,
- Type communications (e.g., dedicated vs. common), and
- Ease of use (human engineering characteristics).

c. Signal Processing

- Time,
- Transmission (hardwire, RF, audio, etc.),
- FAR, and
- Error rates and characteristics.

d. Human Factors

- Vigilance,
- Visual perception capabilities,
- Time-stress factor,
- Circadian factor, and
- Level of training and experience.

4. Operational Characteristics of Reaction

a. Automatic Intrusion Denial Devices

- Probability of incapacitation,
- Time for 100% effectiveness,
- Effective time of incapacitation,
- Probability of fail-safe,
- MTBF, and
- Reliability of initiation.

b. Decision Processing

- Time from decision to implementation,
- Reliability of transmission/receipt of decision, and
- Complexity of decision (number of elements, e.g., guards, armament, denial devices, etc.).

c. Guard Forces

- Response time,
- Means of communication,
- Level of training, and
- Procedures.

5. Operational Characteristics of Neutralization

a. Detaining Systems

- Capacity, and
- Delay times caused by reaction force or barriers.

b. Disabling Systems

- Capacity,
- Disablement means (type, e.g., passive-manipulation of sensory perception or cognitive processes; active-physical disablement), and
- Performance effects produced.

c. Defeating Systems

- Capacity,
- Temporary or reversible: duration of effects,
- Permanent or irreversible: lethal area coverage, probabilities of kill, and
- Boomerang effects (effects on neutralization if used against defenders).

d. Guard Forces

- Friendly *vs.* intruders strength ratios (size, firepower),
- Sustainability, and
- Reinforcement capability.

C. DATA SOURCES

1. General

Operational characteristic data as described in the previous section may be viewed as the "raw material" upon which the SNWS MOE methodology operates. In particular, the values which the FMOE probabilities take for candidate SNWS systems will depend on the operational characteristics of those systems. For this reason, it is important to identify sources of operational characteristic data, which is the purpose of this section.

The four principal sources for such data are:

- Test and Evaluation,
- Manufacturer's Specifications,
- Ongoing Security System Programs, and
- Human Factors Analysis.

2. Test and Evaluation

The nature of operational characteristic data is such that tests to obtain it are relatively easy to design and perform. It is in this sense that the operational characteristics listed above are described as being directly "measurable." The characteristics listed may be measured in operational tests, field tests, laboratory tests, bench tests, and simulations. In most cases, statistical analysis will be required to draw conclusions from the sample data obtained. Finally, the Shipboard Environmental Simulation Facility (SESF) being developed for the SNWS program should provide an ideal test bed for generation of operational characteristic data.

3. Manufacturer's Specifications

Commercial equipment/hardware is developed against required specifications. These specifications are matched to operational requirements for a particular system or subsystem. Hardware being developed in response to a specific government requirement will be designed to meet government technical specifications. Adherence to technical specifications is assured through a series of design reviews and acceptance tests. The SNWS MOE methodology will be able to tap this source for specific operational characteristic data.

4. Ongoing Security System Programs

The Department of Defense has several ongoing security system programs which can provide a major source of data. Major programs include:

- U.S. Army Facility Intrusion Detection System (FIDS),
- Joint Service Interior Intrusion Detection System (JSIIDS),
- Defense Nuclear Agency Forced Entry Deterrent System (FEDS),
- U.S. Air Force Base Installation Security System (BISS), and
- U.S. Navy Waterborne Intrusion Detection System (WIDS).

Relevant human behavior and human engineering data is or will be available from physical security efforts being conducted by the Defense Nuclear Agency (DNA) and the Naval Personnel Research and Development Center (NPRDC) as well.

5. Human Factors Analysis

Of all the elements in the SNWS problem, the most variable, yet least understood, is the human component. The purpose of this discussion is to present a conceptual approach to the design of research programs aimed at the reduction of human component variability. In the area of human factors, successful research programs must be based on a systematic, highly structured rationale. The underlying rationale for successful program development is based upon a three phase program construction technique. These three phases are a mission directed literature review, field testing, and development of a mission-oriented return-on-investment (ROI) metric.

The literature review phase would serve to identify critical problem areas and current remedial technologies in regard to human factors in shipboard nulcear weapon physical security. The field test phase would further define the problems while assessing the effectiveness of various solution methodologies. The ROI metric would relate the cost of pursuing various remedial technologies to the return on investment, in terms of increased security effectiveness and potentially significant financial savings. This balanced approach would yield a prioritized, annotated compilation of proposed investigations into selected human factor issues in physical security.

The literature review phase of program development requires the establishment of search boundaries in terms of time, sources, and subject areas. Example subject areas which relate human factors to physical security include human vigilance, perceptual capability (visual and auditory), visual enhancement technology, information processing under stress, effects of psycho-social variables, vigilance and detection training, motivation research, fatigue/boredom, and circadian symptoms. Once the problem areas and available behavioral technologies have been identified, the next step

would be to define the problems in detail and refine the available remedial strategies. This is best accomplished using field test techniques.

Field testing could be conducted using scenarios developed for SNWS system tests. The test site should be some specially constructed environment built to simulate specific ship types. This simulator could be fitted with Low Light Level TV (LLL TV), audio, vibration sensors, and other types of data collection equipment which feed directly into a small microcomputer, dedicated to on-line data analysis. The results of the field tests would be utilized to establish independent variables for future study, and to validate the MOE provided by the present research. In addition the results from field testing would provide the data base upon which to build a framework to help predict relationships between selected human factors issues and measures of physical security effectiveness.

Once the areas of research have been refined to the desired level of specificity, a ROI metric can be developed. The purpose of the ROI metric is to prioritize the list of research programs in terms of cost, in order to implement and develop potential improvements in the area of security effectiveness. The product of this effort would be a series of systematically constructed research programs, prioritized with regard to the ROI. Each of the programs would be based on analytical data from the literature review, empirical data from the field testing, and cost effectiveness data from the ROI metric.

D. EVALUATION OF FMOE PROBABILITIES

1. General

The capability to determine FMOE probability values for candidate SNWS systems is crucial to the application of the SNWS MOE methodology. Not only are the probabilities for detection, assessment, reaction, and neutralization useful MOEs in their own right, but they are also needed to construct combined MOEs for total security. (These combined MOEs are defined in Chapters 5 and 6.)

This section outlines how the relationship between operational characteristic data and FMOE probabilities may be established and describes means for determining FMOE probability values.

2. Evaluation of FMOE

As defined in Chapter 3, the FMOE for SNWS systems are the conditional probabilities of detection, assessment, reaction, and neutralization. Values of these probabilities for an SNWS system under evaluation serve as the basic measures of that system's effectiveness in performing security functions. But the effectiveness of an SNWS system will be contingent upon the externally imposed security requirements it is supposed to satisfy and the internally imposed requirements which the system imposes on itself for proper operation. (An example of the latter is the situation in which an SNWS system's reaction time is such that for the total system to succeed, detection and assessment must be accomplished within a certain time limit.) These considerations lead to the following important conclusion:

> Determination of FMOE probability values must take into account various "threshold criteria" which are relevant to the SNWS system under evaluation.

These "threshold criteria" are considered by expressing the FMOE probabilities in the following ways:

- P_D = the probability of detection within x minutes of entry into zone or within y meters of boundary of interest
- P_A = the probability of assessment to a prescribed level of detail within x minutes
- P_R = the probability of reaction consisting of a prescribed level of delay-time and/or force strength within x minutes
- P_N = the probability of neutralization of a specified type or degree; e.g., detainment for x minutes or disablement of y% of the threat.

The event specifications are example threshold criteria. The parameters in the threshold criteria will vary depending on the systems being evaluated and the particular SNWS problem area at hand, of course. The key point is

that these threshold criteria may be obtained directly from externally imposed SNWS requirements and/or internally imposed inherent system requirements for proper functioning.

An additional and important benefit follows from the use of threshold criteria in the formulation of FMOE probabilities. Because they serve to define the events of detection, assessment, reaction, and neutralization in precise, quantifiable terms, the threshold criteria make the determination of FMOE probability values much easier. In particular, the relationships beteen operational characteristic data and FMOE probabilities, and the means for evaluating FMOE, become much easier to describe.

3. Operational Characteristic Data and FMOE

Determination of FMOE probabilities based on operational characteristic data may be accomplished in two ways: empirically or through modeling.

Empirical determination would involve testing followed by regression analysis to determine how FMOE values depend on operational characteristic data. Because regression analysis would require determination of sample FMOE values, this approach is most appropriate when extrapolation is required. An example of such extrapolation would be, for instance, an estimate of P_A for a system possessing a certain false alarm rate, based on known assessment probabilities for systems with different false alarm rates.

Modeling provides an alternative (and generally cheaper) way to relate FMOE probabilities and operational characteristic data. In the modeling approach, FMOE probabilities are expressed as mathematical functions of operational characteristic data variables. For example, a reasonable model for the probability of detection is:

$$P_D = 1 - e^{-kt}$$

where t = time and k is a parameter which depends on the threshold criteria for P_D. The graph of this model shows why it is "reasonable" (Figure 4-1). The graph illustrates model representation of the fact that as time goes by the probability that an intrusion attempt will be detected increases asymptotically to one. However, the modeling approach usually requires that

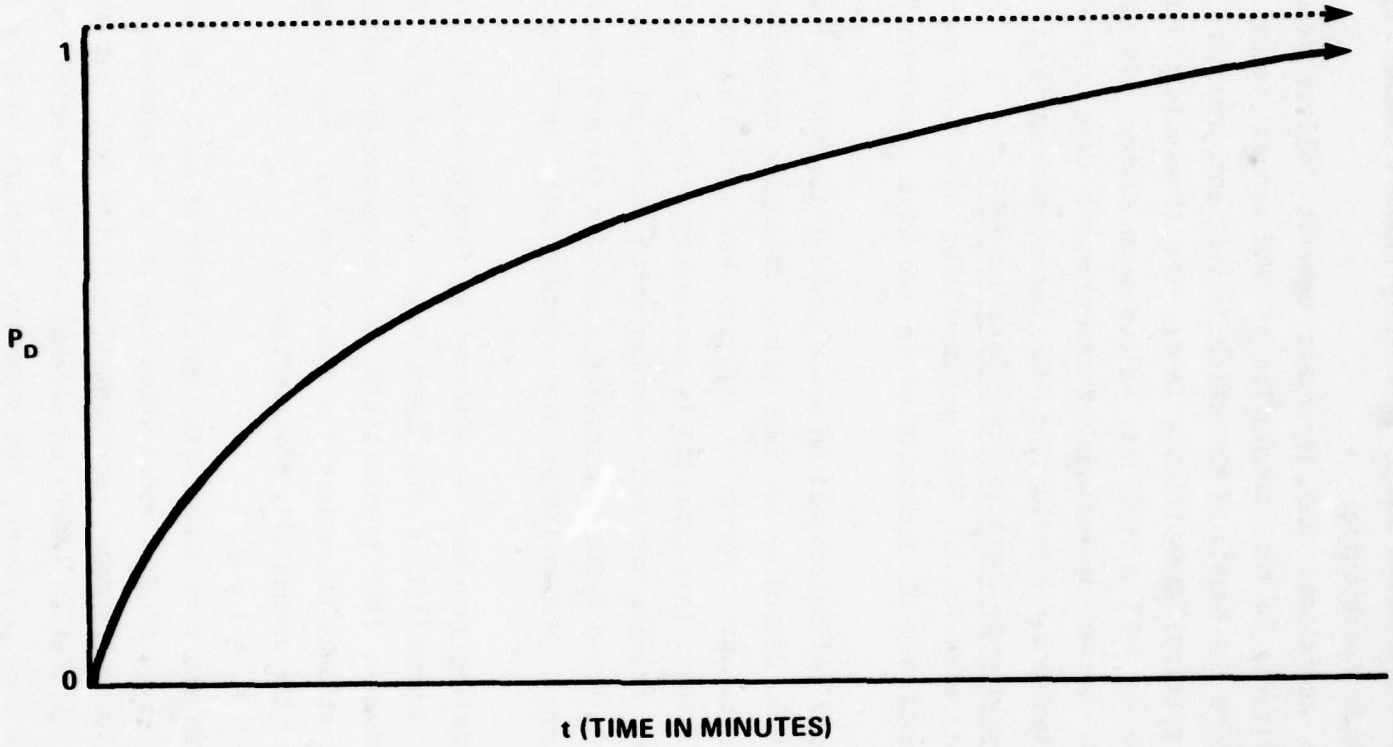


Figure 4-1. Graph of $P_D = 1 - e^{-kt}$

"simplifying" assumptions be made if the models are to be at all manageable. In the absence of empirical validation, however, these assumptions, and the models which result, may bias the methodology. In any case, to apply the models in determination of FMOE values, it would be necessary to obtain test data for the model parameters.

4. FMOE and the SESF

The decision to express the functional measures of effectiveness for SNWS systems as probabilities is a result of the requirement for generality in the SNWS MOE methodology. (The generality requirement exists due to the diversity of the SNWS problem.) In addition, the use of probabilities facilitates the formation of combined MOE for total security (see Chapters 5 and 6).

Probabilities have the disadvantage of being difficult to evaluate. For the SNWS program, however, the problem of determining FMOE probability values is mitigated considerably by the fact that the SESF will be available. By providing the capability to perform repeated trials of different types of penetration attempts against candidate SNWS systems aboard different ship types, the SESF will make it possible to determine FMOE probabilities directly. This capability will make the SESF an ideal test bed for generation of data suitable for use in the SNWS MOE methodology.

CHAPTER 5
COMBINED MOE FOR TOTAL SECURITY

A. INTRODUCTION

The purpose of this chapter is to describe how the functional MOE (FMOE) defined in Chapter 3 may be combined to obtain MOE expressions for evaluating total SNWS system effectiveness, for a given ship type and operating mode. These FMOE are:

- P (detection) = P_D
- P (assessment) = P_A
- P (reaction) = P_R
- P (neutralization) = P_N

The means by which the methodology incorporates the varying security requirements which may exist for different zones of interest is addressed. The methodology as described is not ship type, weapon, operating mode, or threat specific. That is, the algorithms presented for computing combined MOEs are independent of any assumptions in these areas. The data upon which these algorithms work will vary for these different situations, however.

The chapter includes sample calculations with nominal data to illustrate how combined MOE for overall security may be formed.

The chapter concludes with a discussion of how these combined MOE for overall security may be applied, both to system evaluation and system design problems at the level of a single ship. Chapter 6 will describe extended applications of the methodology to these problems at the fleet level.

B. COMBINATION OF FMOE WITHIN ZONES

For the purposes of this section it will be assumed that actual values for the conditional probabilities P_D, P_A, P_R, and P_N are available for a candidate SNWS system aboard a given ship type carrying nuclear weapons in

a given operating mode. (Chapter 4 described means by which these values may be obtained.) In particular, it is assumed that each of these probabilities is known for the security system under evaluation in each of the four zones of interest: off the ship, on board, weapon control/access spaces, and weapon storage spaces. The values for these FMOE probabilities are important because each of the functions of detection, assessment, reaction, and neutralization may apply in each of the zones, depending on the makeup of the security system and the ship type and operating mode being examined.

The probabilities above are determined as conditional by zone. That is, in a given zone P_D represents the probability of detection to a specified degree, P_A denotes the probability of correct assessment (to a specified degree) given detection, P_R denotes the probability of correct and timely reaction (to a specified degree) given correct assessment, and P_N denotes the probability of neutralization (to a specified degree) given a correct and timely reaction. It is possible that one or more of these probabilities is zero for a given zone, if it is the case that in that zone absolutely no capability exists for performance of the corresponding function. For example it may be that no detection capability is provided for a certain ship type exterior zone. In that case P_D would effectively be zero.

As conditional probabilities the FMOEs may be multiplied to obtain the probability of the joint event:

> detection and correct assessment and appropriate reaction and effective neutralization.

If and only if all four of these functions are successfully performed in a given zone can it be said that full and sufficient security is provided in that zone. This may be put another way by saying that if any one or more of these functions is not successfully performed, then security in that zone is effectively non-existent. It should be noted that the assumption is being made that in a given zone if any one function fails to be performed, then it is virtually impossible for subsequent functions to be successfully performed. For example, neutralization cannot take place

unless an appropriate and timely reaction of some sort occurs previously. (There is always the chance that neutralization occurs due to random events for which the SNWS system and personnel can take no credit, e.g., the penetrator has a heart attack, but these events are assumed to have negligible likelihoods of occurrence.) It should also be noted that it is possible for a particular function (e.g., detection) to be successfully performed in a given zone, without having full security. This is because full security is defined to be the integrated performance of all four of the functions of detection, assessment, reaction, and neutralization.

With these definitions, the product

$$P_D(z) \times P_A(z) \times P_R(z) \times P_N(z) = P_{sec}(z) \text{ for } z = 1,2,3,4 \qquad (5\text{-}1)$$

provides a measure of effectiveness for the security provided in each of the four zones of interest. P_{sec} for each of these zones provides the first example of a combined MOE for overall security because it incorporates all four of the functions which security systems perform. Applications of equation (5-1) are discussed in Section F of this chapter.

The next step in developing combined MOE for SNWS involves combining the P_{sec} terms for each zone into an MOE expression for total ship SNWS.

C. COMBINATION OF ZONE SECURITY MOE FOR TOTAL SHIP SNWS MOE

With the assumptions discussed below, the P_{sec} terms for each zone may be combined to obtain an expression P_{SEC} for the probability that full and sufficient security is provided for shipboard nuclear weapons aboard a given ship type in a given operating mode:

$$P_{SEC} = 1 - \prod_{z=1}^{4} \left(1-P_{sec}(z)\right) \qquad (5\text{-}2)$$

P_{SEC} is the second example of a combined MOE for total shipboard nuclear weapon security. A computed value for P_{SEC} as defined by equation (5-2) represents a quantitative measure of a total ship security system's effectiveness in denying access to or control of shipboard nuclear weapons. The reasoning behind equation (5-2) is that in order for a ship's SNWS system to fail, it is necessary that security fail in all four zones. Put another way, if detection, assessment, reaction, and neutralization are successfully accomplished in at least one zone, then access to or control of a nuclear weapon has been denied. The probability that security fails in all four zones is represented by the product term in equation (5-2). One minus this product is therefore the probability that security is provided in at least one zone, or equivalently, that full and sufficient security is provided by the total ship SNWS system.

In order for the product term in equation (5-2) to accurately represent the probability that security fails in all four zones, it is necessary to assume that the likelihood that security is maintained in any one zone is independent of whether or not security is maintained in any other zone. This assumption is justified by considering a "worst case" situation in which it is assumed that a threat to shipboard nuclear weapons may originate in <u>any</u> of the four zones of interest. This situation is not unreasonable given assumptions about "insider" participation across the threat spectrum.

Also related to the independence between zones assumption is a question concerning interconnections between zones in the four functional areas. It may be the case, for example, that a given security system is designed so that detection would be accomplished in one zone and this information passed to another zone for purposes of assessment. In order to allow for this possibility, it is necessary that some care be taken to gather functional MOE data which is appropriate for use in computing P_{SEC}. Because P_{SEC} is meant to serve as a <u>combined MOE</u> for a <u>total ship SNWS system</u>, it is important that the zonal FMOE data gathered reflect performance of the <u>total</u> system in operation and not just selected components. While this does complicate test planning, it is a necessary complication,

because full and complete evaluation of an SNWS system will require that the system be tested in toto as an integrated operational entity.

P_{SEC}, as defined by equation (5-2), is a measure of total SNWS system effectiveness which reflects the defense-in-depth effects provided by the zones surrounding shipboard nuclear weapons. Applications of P_{SEC} and equation (5-2) are discussed in Section F of this chapter. The next section describes a second combined MOE for total ship SNWS, different from P_{SEC}, which reflects the fact that different zones may have different levels of importance for security from ship type to ship type or from one operating mode to another.

D. ZONE WEIGHTING AND THE SECURITY INDEX

As noted in Chapter 2, a unique characteristic of the SNWS problem is that the relative importance of maintaining security in the different zones surrounding shipboard nuclear weapons may vary with ship type, operating mode, and the nature of the weapons to be protected. On an SSBN in port, for example, keeping unauthorized personnel from boarding (i.e., penetrating zone 2) is important, both from the standpoint of SNWS and from that of total platform security. On an aircraft carrier in port however, zone 2 security is probably less crucial, given the different shipboard nuclear weapon locations aboard carriers, as well as practical considerations which make zone 2 security for a CV in port unrealistic.

Because the relative importance of providing security in different zones may vary, it is desirable to have an MOE for total ship SNWS which will reflect how well systems provide security in those zones where it is most needed or most important. P_{SEC}, as defined in the previous section, does not do this because implicit in its construction is the defense-in-depth idea that all zones are of equal value in providing total security. The rationale there is that if the threat is neutralized in any one zone, then the SNWS system has accomplished its goal.

A combined MOE which does reflect the relative importance of zonal security is constructed as follows:

Let w_z for z = 1, 2, 3, 4 be a number between 0 and 1 which represents the relative importance (or desirability) of stopping a threat to SNWS in zone "z" for a given ship type in a given operating mode. These zone weighting factors, because they are measures of relative importance, are assigned values so that they sum to one:

$$\sum_{z=1}^{4} w_z = 1$$

For a given ship type/operating mode the w_z are fixed weights, but their values may (and will) vary for different ship types and operating modes. Even for the same ship type there may be different w_z values for different operating modes; e.g., the relative importance of security decreases in zones 1 and 2, and increases in zones 3 and 4, for an SSBN when it transitions from in port to underway.

These zone weighting factors can now be combined with the zonal $P_{sec}(z)$ terms defined in Section B to obtain a security index (SNWSI):

$$SNWSI = \sum_{z=1}^{4} w_z \, P_{sec}(z) \qquad (5\text{-}3)$$

The SNWSI for an SNWS system on a given ship type in a given operating mode is a weighted average of the zonal security probabilities, weighted by the relative importance of security in each zone. As such, the security index provides a combined MOE for total ship SNWS which measures how well balanced system performance is, in terms of providing security where it is most needed or desired.

The security index is not a probability. It is possible, for instance, that for a given ship type and operating mode two different SNWS systems would produce different security indices but the same overall probabilities of security (P_{SEC}'s). The difference would be that the

system with the larger security index probably does a better job in providing security where it is most desirable to have it. It is also possible that a candidate security system would result in equal P_{SEC}'s for two different ship types, but different security indices. In this case a conclusion would be that the system is better suited for that ship type in which it scored a higher security index, because this would indicate that, for that ship type, the system is better at providing security where it is needed or most appropriate. Further applications of the security index are discussed in Section F of this chapter.

E. EXAMPLE CALCULATIONS

Figures 5-1 and 5-2 illustrate calculations of combined MOE for total ship SNWS based on nominal values for functional MOE in each of the four zones. The calculations are done for two different ship types (CV and SSBN) in port to illustrate a situation in which overall probabilities of security (P_{SEC}) are the same, but security indices differ.

A conclusion which could be drawn from the results of the calculations is that even though the security systems for the CV and the SSBN both result in a high probability of providing effective overall SNWS, the CV's system is a better system in terms of how and where it does its job.

F. APPLICATIONS

This section describes possible applications of the combined MOE for SNWS defined above:

- $P_{sec}(z)$ (probability of security in zone z - eq. 5-1)
- P_{SEC} (probability of overall SNWS - eq. 5-2)
- SNWSI (security index - eq. 5-3).

Each of these MOE take values between 0 and 1, and each may be used to assess aspects of system performance aboard a given ship type in a given operating mode. (Combined applications of these measures across the fleet are discussed in the next chapter.)

IN PORT

	ZONE			
	OFF SHIP Z=1	ON BOARD Z=2	WEAPONS SPACE Z=3	WEAPON Z=4
DETECTION (P_D)	0.05	0.50	0.995	0.995
ASSESSMENT (P_A)	0.80	0.60	0.999	0.999
REACTION (P_R)	0.95	0.90	0.98	0.999
NEUTRALIZATION (P_N)	0.50	0.50	0.90	0.75
SYSTEM $P_{sec}(z)$ $=P_D(z)xP_A(z)xP_R(z)xP_N(z)$	0.019	0.1425	0.876	0.744
ZONE WEIGHT W_z	0	0.05	0.85	0.10

$$\text{SECURITY INDEX} = \sum_{z=1}^{4} W_z\,[P_{sec}(z)] = .8268 \qquad P_{SEC} = 1 - \prod_{z=1}^{4} \left(1 - P_{sec}(z)\right) = .9736$$

Figure 5-1. CV - Example Calculation

IN PORT

	ZONE			
	OFF SHIP Z=1	ON BOARD Z=2	WEAPONS SPACE Z=3	WEAPON Z=4
DETECTION (P_D)	0.1	0.9	0.2	0.9
ASSESSMENT (P_A)	0.95	0.8	0.99	0.999
REACTION (P_R)	0.999	0.99	0.95	0.995
NEUTRALIZATION (P_N)	1	0.95	0.75	0.95
SYSTEM $P_{sec}(z)$ $=P_D(z)xP_A(z)xP_R(z)xP_N(z)$	0.0949	0.683	0.141	0.891
ZONE WEIGHT W_z	0.05	0.80	0.05	0.10

$$\text{SECURITY INDEX} = \sum_{z=1}^{4} W_z\,[P_{sec}(z)] = .6475 \qquad P_{SEC} = 1 - \prod_{z=1}^{4} \left(1 - P_{sec}(z)\right) = .9731$$

Figure 5-2. SSBN - Example Calculation

For each of the combined MOE, applications are discussed in terms of the two major application areas for the SNWS MOE methodology:

- the system evaluation problem, and
- the system design problem.

The SNWS MOE methodology is applied to the system evaluation problem to assess the effectiveness of candidate systems. In this application the SNWS MOE methodology can be used to compare the performance of competing systems or to compare a single system's performance to specified requirements. The methodology may also be applied to the system design and requirements specification problem, however, in that it supplies a systematic means for developing quantitative criteria to serve as guides for development of candidate systems.

1. Applications of Zonal Probability of Security

The probability of full and sufficient security in a given zone, $P_{sec}(z)$, may be used to evaluate and compare components of total ship SNWS systems which are specifically designed to serve in particular zones. For example, if it were desired to compare two waterborne intrusion detection systems (WIDS) of differing design, then $P_{sec}(1)$ would be an appropriate measure. This application is particularly relevant if circumstances require that components be evalauted in isolation, as opposed to being evaluated as integrated elements of a total ship SNWS system.

$P_{sec}(z)$ may also be used to develop performance requirements for zonal SNWS components in each of the four functional areas. Given upper bounds, for instance, on system capacity to provide for assessment, reaction, and neutralization in a given zone, then equation (5-1) may be used to compute the minimum probability of detection required to meet an overall zonal security specification.

2. Applications of Ship Probability of Security

The probability of full and sufficient SNWS aboard a given ship type in a given operating mode, P_{SEC}, may be used to evaluate and compare the performance of total SNWS systems, because it is computed (equation 5-2) from data which reflect component performance in all four functional

areas across all zones of interest. P_{SEC} is particularly useful in comparing a given system's performance to specified requirements, because these requirements are often stated in terms such as "98% assurance that no unauthorized personnel gain access to or control of an shipboard nuclear weapon", and P_{SEC} is defined to provide an MOE which may be expressed in precisely these terms. P_{SEC} may also be used in conjunction with cost information to analyze cost vs. performance tradeoffs.

P_{SEC} may also be used to develop performance requirements for purposes of total system design. Given practical constraints on the level of security which can be achieved for an inport CV in zones 1 and 2, for example, equation (5-2) can be solved for $P_{sec}(3)$ and $P_{sec}(4)$ to determine how security in zones 3 and 4 must be balanced to achieve a given assurance level for overall security.

3. Applications of the Security Index

Various ways in which the security index may be applied to the system evaluation problem are discussed in Section D. The following discussion illustrates, in addition, how cost/performance tradeoffs can be examined using the security index as a figure of merit.

Figure 5-3 illustrates how the security indices for (eight) candidate systems could be plotted against the costs associated with those systems. The dotted line indicates a minimum acceptable security index for the ship type/operating mode in question. With this information, one could elect to choose that system (circled) which meets the minimum acceptable requirement and has lowest cost. Alternatively, those systems which meet the minimum acceptable requirement and are within budget constraints could be ranked by unit cost (security index/cost) or by percent increase in security index vs. percent increase in cost (with respect to the circled system). Similar cost-benefit analyses, using P_{SEC} in place of the security index, could also be performed in this way.

G. QUANTITATIVE TECHNIQUES FOR ZONE WEIGHTING

The zone weights used in the calculation of a security index have significant bearing on the index's final value. As indicators of the

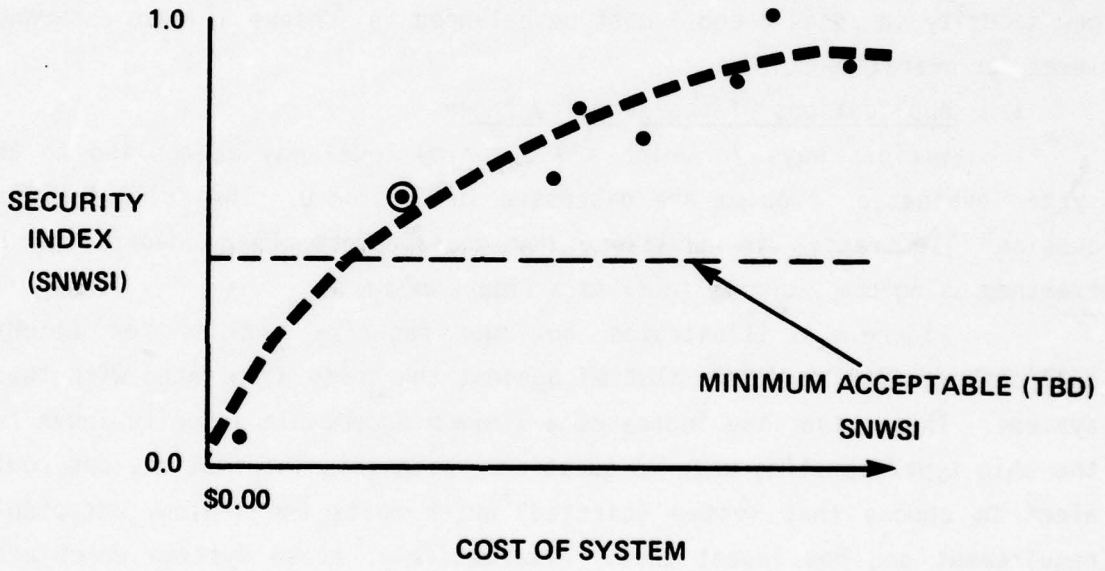


Figure 5-3. Security Indices vs Costs

4508/78W

relative importance of providing security in the different zones, these weights are not directly measurable quantities, however. For this reason it is important that these weighting factors, which are essentially subjective in nature, be determined in a controlled and systematic way. The purpose of this section is to describe a methodology to establish quantified rankings for relative importance of each security zone's contribution to SNWS.

The principal reason for zonal weightings is to provide a means by which the different physical configurations of Naval platforms, and their inherent unique security requirements, can be mathematically modeled in the SNWS MOE methodology.

An additional benefit of a zone weighting methodology is that it can be used in the context of the system design problem. It may be that all zones do not require all security functions to be performed, or that certain zones are not critical to the protection of particular shipboard nuclear weapons. By providing only the required zonal security, budgetary constraints could be satisfied or costs minimized by procuring only those SNWS systems required to meet operational requirements.

In order to develop criteria for optimal security the first step is to develop reliable estimates of the relative criticality of shipboard security zones. Such estimates are, by their nature, subjective. Nevertheless, reliable and useable estimates may be obtained by applying proven techniques from the psychological studies of attitude measurement to quantify the specific attitudes of selected Naval shipboard security experts. The approach is described below.

The attitude measurement approach requires two basic elements: first, the careful selection of a representative panel of experts; and second, the development of an objective attitude assessment technique. Systematic implementation of these elements will produce empirically based, reliable indices of security zone criticality, which can be used to weight zones in security index calculations. Additionally, the zonal weights can be used as a diagnostic tool to identify zones which require improved security.

The approach to solve the problem of zone weighting begins with the establishment of a "Delphi Panel", which consists of a group of experts. In order to properly select this group, it is first necessary to establish parameters for the selection process. Example selection parameters might be: expertise in shipboard security, operational experience in covert operations, extensive Naval experience, familiarity with SNWS nuclear weapon operations, etc. Next a representative number of panel members must be chosen to obtain the necessary reliability. In general, when selecting expert panels the number of members required is inversely related to the level of sophistication or expertise among the individual members. Previous studies employing Delphi panels have shown that as more and more panel members are added, less and less new information on any specific topic is gained. With very experienced personnel, the amount of new information added becomes insignificant when the panel size exceeds 10. Once the parameters and panel size are known, selection procedures can be applied to the available population of potential members.

While panel selection is taking place, work can begin on the development of the attitude measurement techniques. There are numerous techniques for the assessment of attitude including: survey questionnaires, telephone interviews, personal interviews, role playing, focus groups, etc. A combination of these techniques is recommended in order to maximize effectiveness. One potential method is to consider the panel of experts as a focus group and to provide a scenario which sets the stage for a covert intrusion aboard a specific ship type by a specific threat. The focus group could be shown a videotape or could listen to an audio scenario. Then each panel member would be requested to write or dictate his plan for establishing control of the nuclear weapon. This plan would be content analyzed for the frequency and intensity of statements regarding various zones of security. Following this narrative each panelist could then be given a separate structured interview, specific to the concept of zone weighting. Each panelist could be asked to rate the importance of detection within each security zone. Each could also be asked to rank order the security zones with respect to security functions performed by zone. An example of how

this question could be phrased is: "In regard to control of shipboard nuclear weapons, please rate the importance of detecting an intruder in security zone z by placing a / on the line:"

NOT IMPORTANT ——————————————— VERY IMPORTANT

Succeeding items would relate to the importance of assessment, reaction and neutralization.

These items would be based on the scenario of interest and would be checked for consistency against the narrative descriptions of intrusion plans given previously.

Once the content analysis results and the rating scale results have been correlated to insure consistency of the statements, they would be ready for further statistical analysis. The product of the statistical treatment would be quantitative measures of importance for each security zone aboard a specific ship type. This information could be made further specific to threat type by devising scenarios which encourage the panelist to play specific roles, e.g., terrorist, fanatic, vandal, thief, etc.

The measured scores for each zone can be computed across panelists and over all response items to establish an overall index of zone criticality or zone weight. In addition, this technique would provide data for the computation of the criticality of any specific security function within any zone. The possible interactions are shown in Figure 5-4. The product of this assessment process will be an empirically determined, reliable indicator of security zone criticality with regard to the functions performed in those zones. This indicator would be used to weight the zones for MOE calculation or to pinpoint areas of necessary security improvement.

THREAT: VANDAL

SHIP: SUBMARINE

SECURITY ZONE	DETECTION	RECOGNITION	REACTION	NEUTRALIZATION
1	FREQ 6 PROB 80 CRIT INDEX 240			
2				
3			FREQ 2 PROB 30 CRIT INDEX 60	
4				

ENTER CELLS WITH MEASURES REFLECTING THE CRITICALITY OF SECURITY FUNCTION X WITHIN ZONE Y. THE ACTUAL NUMBERS IN THE CELLS INDICATE MEAN FREQUENCY AND MEAN PROBABILITY ACROSS ALL PANELISTS FOR EACH FUNCTION.

Figure 5-4. Security Zone Weighting Matrix

CHAPTER 6
FLEET APPLICATIONS

A. INTRODUCTION

The purpose of this chapter is to describe how the combined SNWS MOE defined in Chapter 5 may be applied to the SNWS problem at the fleet level. The MOE described in Chapter 5: $P_{sec}(z)$, P_{SEC}, and the Security Index are all similar in that they each provide a measure of system performance aboard a given ship type in a given operating mode. As there are many different ship types and operating modes involved in the SNWS problem, however, it is natural to ask the following questions:

(1) Assuming one has combined MOE for different security systems by ship type and operating mode, how can these MOE be combined to obtain overall MOE for evaluating systems for the fleet?

(2) How can combined SNWS MOE be applied to the system design problem across the fleet, taking cost considerations into account?

This chapter describes techniques which address both of these questions.

For purposes of answering the first question, the security index MOE will be used to describe how a combined SNWS MOE may be applied to the system evaluation problem at the fleet level. The technique described does not combine security indices into an overall MOE as such, but rather applies standard non-parametric statistical techniques to determine overall results.

The method described may be applied to the combined MOE for zonal security, $P_{sec}(z)$, and the MOE for total security, P_{SEC}, as well. (The technique may also be applied using the MOE for deterrence described in Chapter 7.)

To answer the second question, the combined MOE for zone and ship security are used to obtain parameters for constrained optimization problems which consider costs and which can be solved to determine optimal system configurations.

B. THE SYSTEM EVALUATION PROBLEM AT THE FLEET LEVEL

1. Problem Definition

It is unlikely that a single SNWS system will be capable of handling the SNWS problem across the entire fleet. It is possible, however, that different combinations of components drawn from a fixed set of available systems will be used to provide "different" security systems which are "tailored" to various ship types. It is also possible that within the fleet there are subsets of different ship types which nonetheless possess sufficiently similar shipboard nuclear weapon environments to justify attempts to identify a single overall SNWS system which could be used aboard each type. Even for a single ship type, it may be the case that different SNWS systems are required to maximize security in each of the three possible operating modes. Regardless of which of these situations applies, it would be useful to have a technique for determining which is the "best" of several candidate systems or configurations, given various performance levels for the systems across different ship types or operating modes.

Given a set of candidate SNWS systems for possible use aboard a collection of various ship types, it is possible to determine a security index for each pair of the form (ship type, security system). An example of the resulting matrix of security indices is illustrated (using nominal values) in Figure 6-1. In Figure 6-1, there are four candidate SNWS systems (labeled 1, 2, 3, and 4) and seven ship types of interest. Within each row of the matrix, the security indices achieved by the four systems for that row's ship type are ranked according to magnitude (ranks in parentheses), with the highest security index receiving the rank of 4, the next highest 3, and so on. Row-by-row inspection of the ranks shows that, using the security index as the measure of effectiveness, different systems do the "best" job for different ship types, with the result that no one system stands out clearly as being better than the others.

2. Problem Solution

The problem described above may be solved through the use of standard non-parametric (distribution-free) statistical techniques. In

SECURITY INDICES
(RANKS)

SHIP TYPES	CANDIDATE SNWS SYSTEMS			
	1	2	3	4
AS	.790 (3)	.815 (4)	.700 (2)	.615 (1)
AD	.655 (3)	.712 (4)	.594 (2)	.577 (1)
AE	.850 (2)	.915 (4)	.887 (3)	.775 (1)
AO	.570 (2)	.290 (1)	.715 (4)	.703 (3)
AOE	.667 (2)	.812 (4)	.777 (3)	.590 (1)
CV	.827 (4)	.725 (2)	.810 (3)	.702 (1)
SSBN	.648 (4)	.241 (1)	.275 (2)	.503 (3)

Figure 6-1. Security Index Matrix

particular, a non-parametric hypothesis testing algorithm, known as the Friedman Two-Way Analysis Distribution-Free Test* may be applied. In this application one tests the null hypothesis that all four security systems result in equal security for the seven ship types. The alternative hypothesis is that the security levels provided by the four systems across the various ship types are not all the same. As is the case in any hypothesis test, the probability of Type I error is controlled through the choice of significance level. In this application, a Type I error would be to reject the hypothesis that the four systems provide equal security when, in fact, they do.

Figures 6-2 through 6-3 illustrate the application of the Friedman test to the data in Figure 6-1. At the .05 significance level the hypothesis that the four candidate systems provide equal security is accepted. This conclusion would allow a decision-maker to use other criteria (cost or deterrent effects, for example) as a basis for decision.

Figures 6-4 through 6-6 illustrate the application of the Friedman test to another set of (nominal) security index data. In this example, the equal security hypothesis is rejected at the $\alpha = .05$ level. When the null hypothesis is rejected, another non-parametric test, Multiple Comparisons Based on Friedman Rank Sums**, may be applied to determine which "treatment" (security system) is the best overall. In the example shown in Figures 6-5 and 6-6, we conclude that security system 2 is the best overall for the ship types considered, with an experiment-wise error rate (similar to significance level) of .032. In non-technical terms, we can say with very high confidence that security system 2 provides significantly better security across the seven ship types than any of the other candidate systems.

In general, the statistical methods described above may be used to solve the SNWS system evaluation problem in any situation in which there

---

* A detailed description of the basis for this test may be found in Hollander and Wolfe, Nonparametric Statistical Methods, Wiley 1973, pgs. 138-158.

** Details may be found in Hollander and Wolfe, op. cit.

TO TEST: H_o: $T_1 = T_2 = T_3 = T_4$ (SECURITY SYSTEMS) AGAINST THE ALTERNATIVES THAT THE T's ARE NOT ALL EQUAL

PROCEDURE:

1) WITHIN EACH BLOCK (SHIPTYPE), RANK THE K OBSERVATIONS FROM LEAST TO GREATEST. LET r_{ij} DENOTE THE RANK.

2) SET $R_j = \sum_{i=1}^{n} r_{ij}$ n = # OF BLOCKS (SHIP TYPES)
k = # OF SECURITY SYSTEMS (TREATMENTS)

3) COMPUTE $S = \left[\frac{12}{nk(k+1)} \sum_{j=1}^{k} R_j^2 \right] - 3n(k+1)$

4) AT THE α LEVEL OF SIGNIFICANCE

REJECT H_o IF $S \geq s(\alpha,k,n)$

ACCEPT H_o OTHERWISE

VALUES FOR $s(\alpha,k,n)$ OBTAINED FROM NONPARAMETRIC STATISTICAL METHODS BY HOLLANDER & WOLFE (TABLE A.15)

Figure 6-2. The Friedman Hypothesis Test

TEST: H_o: $T_1 = T_2 = T_3 = T_4$

H_1: NOT ALL T's ARE EQUAL

$R_1 = 20$

$R_2 = 20$

$R_3 = 19$

$R_4 = 11$

$$S = \left[\frac{12}{(7)(4)(5)} \sum_{j=1}^{4} R_j^2 \right] - 3(7)(5)$$

$$= 4.885$$

$S(.052, 4, 7) = 7.629$

$S(.10, 4, 7) = 6.257$

$S(.195, 4. 7) = 4.886$ $\qquad$ $S(.220, 4, 7) = 4.543$

AT α = .05 OR .10 WE ACCEPT H_o → NO DIFFERENCE IN SECURITY SYSTEMS

SINCE $S < s(\alpha, k, n)$

WE WOULD HAVE TO ALLOW A SIGNIFICANCE LEVEL OF .195 IN ORDER TO REJECT H_o

Figure 6-3. Test Results

SECURITY INDICES

(RANKS)

SHIP TYPE	CANDIDATE SNWS SYSTEMS			
	1	2	3	4
AS	.775	.720	.615	.706
	(4)	(3)	(1)	(2)
AD	.532	.735	.594	.698
	(1)	(4)	(2)	(3)
AE	.887	.837	.792	.803
	(4)	(3)	(1)	(2)
AO	.623	.703	.590	.270
	(3)	(4)	(2)	(1)
AOE	.708	.812	.537	.725
	(2)	(4)	(1)	(3)
CV	.832	.912	.829	.936
	(2)	(3)	(1)	(4)
SSBN	.503	.648	.314	.275
	(3)	(4)	(2)	(1)
	$R_1 = 19$	$R_2 = 25$	$R_3 = 10$	$R_4 = 16$

Figure 6-4. Security Index Matrix

TEST: H_o: $T_1 = T_2 = T_3 = T_4$

H_1: NOT ALL T's ARE EQUAL

$S = 10.029$

$S\ (.052, 4, 7) = 7.629$

$S\ (.012, 4, 7) = 10.029$

AT $\alpha = .012$ WE REJECT H_o → NOT ALL TREATMENTS ARE THE SAME

DISTRIBUTION-FREE MULTIPLE COMPARISONS BASED ON FRIEDMAN RANK SUMS:

CALCULATE THE $\binom{k}{2}$ DIFFERENT COMBINATIONS OF DIFFERENCES

DECIDE $T_u > T_v$ IF $R_u - R_v \geq r\ (\alpha, k, n)$ (TABLE A.17)

$R_1 - R_2 = -6$ $\qquad$ $R_2 - R_3 = 15$

$R_1 - R_3 = 9$ $\qquad$ $R_2 - R_4 = 9$

$R_1 - R_4 = 3$ $\qquad$ $R_3 - R_4 = -6$

$r\ (.008, 4, 7) = 15$ → DECIDE $T_2 > T_3$ AT EXPERIMENT WISE ERROR RATE OF $4\ (.008) = .032$

Figure 6-5. Test Results/Friedman Rank Sums

r (.008, 4, 7) = 15

r (.020, 4, 7) = 15

r (.037, 4, 7) = 13

DECISION: $T_2 > T_3$ → ONLY SIGNIFICANT ORDERING

$T_1 = T_2$

$T_1 = T_3$ (TRANSITIVITY IS

$T_1 = T_4$ NOT A PROPERTY

$T_2 = T_4$ OF THIS TEST)

$T_3 = T_4$

DEFINITION: $T_1 = T_2$ DOES NOT IMPLY TRUE EQUALITY BUT INDICATES THAT T_1 IS NOT SIGNIFICANTLY DIFFERENT FROM T_2, AND IT IS FOR THIS REASON THAT TRANSITIVITY DOES NOT HOLD

DECISION: CHOOSE SECURITY SYSTEM 2 OVER ALL SHIP TYPES (DISREGARDING ANY COST FACTORS)

Figure 6-6. Decision Based on Friedman Rank Sums

are a number of candidate systems being considered for use across a number of different platforms or operating environments. For example, the method could be used to rank order different systems being considered for use in zone 3 (weapon control/access spaces) across a variety of ship types in the fleet. In this case, the appropriate MOE to use as input data for the test would be the various probabilities of security in zone 3 ($P_{sec}(3)$'s) associated with each of the possible ship type/security system combinations.

C. THE SYSTEM DESIGN PROBLEM AT THE FLEET LEVEL

1. Problem Definition

As the SNWS program proceeds, it may develop that different security systems become candidates for use across different ship types in the fleet. These different systems may consist of different sets of components whose functions reflect different approaches to the SNWS problem, or they may just be different combinations or configurations of the same basic set of components. In either case, the system design problem at this level is to determine optimal system mixes for use across the fleet. A system mix could be considered optimal if it maximizes security across the fleet and at the same time satisfies various constraints related to cost and system availability. Alternatively, a system mix could be viewed as optimal if it satisfies various minimum security requirements and at the same time minimizes costs.

2. Problem Solution

The types of problems posed above may be solved through the use of mathematical programming techniques. In particular, system design problems for SNWS across the fleet may be formulated in terms of linear programming problems, with coefficients derived from the combined measures of the SNWS MOE methodology defined in Chapter 5.

Figure 6-7 illustrates how a fleet level system design problem may be formulated as a linear programming problem. The problem illustrated is one in which it is desired that zone 1 security across several different ship types be maximized given a fixed budget and constraints on the number of security systems needed and available or applicable.

	SECURITY SYSTEMS			
	A	B	C	D
COST ($K)	10.2	4.6	9.3	7.5
P_{sec} FOR ZONE 1 (OVERALL)	.109	.054	.083	.067

X_A = # OF SECURITY SYSTEM A

X_B = # OF SECURITY SYSTEM B

X_C = # OF SECURITY SYSTEM C

X_D = # OF SECURITY SYSTEM D

MAXIMIZE OBJECTIVE FUNCTION

$Z = .109X_A + .054X_B + .083X_C + .067X_D$

SUBJECT TO: $10.2X_A + 4.6X_B + 9.3X_C + 7.5X_D \leq$ BUDGET

$X_A + X_B + X_C + X_D$ = # OF OFF-BOARD SECURITY SYSTEMS REQUIRED

$X_A \leq$ # A SYSTEMS AVAILABLE/APPLICABLE

$X_B \leq$ # B SYSTEMS AVAILABLE/APPLICABLE

etc.

(SIMPLEX METHOD)

Figure 6.7. Linear Programming for System Design

The variables in the problem (X_A, X_B, X_C, X_D) represent the number of systems A, B, C, etc. which are to be used. The problem is set up for a situation in which there are four candidate zone 1 security systems. Nominal unit costs for these systems are expressed in thousands of dollars. Associated with each security system is an <u>average</u> value for $P_{sec}(1)$, derived from the zone 1 probabilities of security which that system produces for the different ship types in question. It is necessary that average zonal security probabilities be used because a <u>single</u> coefficient is needed to reflect a given system's performance in zone 1 across several different ship types in the fleet.

The objective function to be maximized is a linear combination of the variables, with the average zonal security probabilities as coefficients. The idea behind the objective function is that the security produced for the fleet is measured by the average security produced using system A, times the number of system A's used, plus a similar term for system B, and so forth.

The cost constraint in the problem is simply the linear inequality which expresses the fact that the total amount spent must be less than or equal to what the budget allows. Another constraint is that the total number of systems used must be equal to the number of systems needed. The final constraints express the fact that there are limits on the number of systems available or applicable. (It may be the case that, due to storage limitations, system A cannot be used on more than 1/3 of the ship types in question, for example.)

Standard techniques (simplex algorithms) exist for solving linear programming problems such as this. The solution to the problem is a set of values for X_A, X_B, X_C, and X_D which maximizes the objective function (fleet security) and satisfies the imposed constraints. These values would represent the optimal mix of systems A, B, C, and D for zone 1 security in the fleet.

Similar linear programming problems can be set up and solved for other possible system design applications of the SNWS MOE methodology at the fleet level.

CHAPTER 7
ADDITIONAL CONSIDERATIONS

A. INTRODUCTION

The purpose of this chapter is to present a discussion of two additional SNWS measures of effectiveness, deterrence and recoverability, and to define their role in the SNWS MOE methodology. The chapter provides recommended application of these MOEs to the assessment of SNWS systems.

B. DETERRENCE

1. Definition

Since the fundamental purpose of an SNWS system is to deny unauthorized access to shipboard nuclear weapons, previous chapters have dealt with classical methods for access denial. An SNWS system's effectiveness, however, may also depend on the system's ability to deter attacks. An SNWS system's effectiveness in providing deterrence is a function of the "psychological barriers" which the system is able to erect in the mind of a potential intruder. Deterrence may be defined as the perception by a potential intruder of the presence of personally negative consequences of his behavior. Deterrence can also be thought of as the potential intruder's perception of the absence of rewarding consequences of his behavior. The key concepts of these definitions are common and, when specifically defined, provide the elements of a deterrence measurement approach. These concepts include:

(1) The specification of the potential intruder,

(2) Definition of perceptual input channels, and

(3) Establishment of positive and negative consequences.

The underlying assumption for all behavioral deterrence studies is that one's knowledge of the results of his behavior will modify that behavior.

The purpose of this section is to describe a conceptual approach to the measurement of the psychological deterrence capability of SNWS systems. The method proposed relies heavily on the literature and methods of social psychology and market research. The approach is described in the following paragraphs.

2. Quantification

The methodology centers around the adaptation of a new attitude measurement and analysis technique developed originally for the purpose of marketing research and advertising. This concept of a deterrence measurement system includes interviews, questionnaires, and computer software designed specifically for studying the attitudes of groups or markets. While this concept originally began as a measurement technique, it logically evolved into a whole technology for collecting and processing attitude information. The end product of this approach provides the capability: to determine the most effective message strategies for influencing threat behavior, to measure the effect that these messages actually have on potential threat attitudes, to simulate effects of various alternative strategies on behavior, and to track attitudes over time.

The first step in conducting a study using this conceptual approach is to determine what descriptors the threat uses to define and evaluate a SNWS system. The purpose is to ensure that all subsequent portions of the procedure are keyed to the thoughts of the target audience rather than the suppositions and biases of either the user or the researcher. This step is accomplished by a series of interviews and focus groups with participants who are representative of the target population.

The focus group should comprise selected, experienced security experts, reaction force participants, experts in infiltration, and experienced Naval personnel. The focus group should be limited to less than 15 individuals and should be used on an iterative basis over time to insure reliability of results. The task of this focus group would be to provide pertinent descriptions of concepts associated with the deterrence effects

of SNWS systems. These concepts would be established by providing the focus group with a series of scenarios which vary threat type and SNWS systems to be breached. The products of this stage would resemble a matrix as shown in Figure 7-1.

The identified SNWS system descriptors should then be included in a questionnaire which pairs them with: each other, the overall concept of physical security, and each of the threat concepts. The threat concept would be a composite attitude/belief structure which most accurately represents the behavioral profile of the specific type of intruder.

The next step would be to administer the questionnaire to a larger sample of the target population. Any of the typical data collection procedures can be used including personal interviews, telephone surveys, or mail surveys. In this case, the target population would be composed of Naval security officers and/or others concerned with SNWS security. Ideally, the respondents should be segmented into groups representing threat types, by providing them with threat related scenarios. These scenarios would give each group a "mental set" related to a specific threat type, such as "political terrorist."

Figure 7-2 presents an example of a typical questionnaire for the sample segment representing the "political terrorist" threat type.

To complete the questionnaire, respondents are provided with a baseline distance and are told to indicate how far apart each concept pair is. For example, respondents could be told that black and white are 100 units apart. Given this baseline, indicate how far apart are the other pairs of descriptors. Figure 7-2 is illustrative since it depicts only three associated descriptors. A full scale study would give many more descriptors and would require the assessment of all possible concept pairs. The use of the distance simulation technique avoids the need to standardize the data prior to analysis, since all responses are based on a common metric, i.e., the baseline distance between concepts.

The only transformation made to the data, prior to analysis, is the averaging of the distances between all respondents' concept pairs. Since this technique measures the interrelationships among all concepts in

Intruder	TARGETS				
	SS	CV	AE	CG	DD
INADVERTENT					
TROUBLEMAKER					
THIEF/VANDAL					
DISAFFECTED CREW					
DERANGED INDIVIDUALS					
DEDICATED, TRAINED, WELL-EQUIPPED PROFESSIONALS					

CELLS WOULD BE FILLED BY DESCRIPTION OF SNWS SYSTEM CONCEPTS WHICH ARE CONSIDERED NEGATIVE BY EACH THREAT CATEGORY.

Figure 7-1. Attitude Matrix

ME = POLITICAL TERRORIST PROFILE. ASSUME THAT BLACK AND WHITE ARE 100 UNITS APART. HOW FAR APART ARE:

DESCRIPTOR	UNITS
EXISTING SNWS AND ME?	40
INJURY AND ME?	50
DEATH AND ME?	90
FAILURE AND ME?	35
SNWS AND INJURY?	.
SNWS AND FAILURE?	.
SNWS AND DEATH?	.

Figure 7-2. Conceptual Deterrence Questionnaire

the data it could theoretically be used to construct maps depicting the relationships between questionnaire items as seen by respondents. An example of such a map is presented in Figure 7-3. The map includes a set of possible descriptors associated with any SNWS system, the specified system under invesgitation, and the assumed threat.

In order to interpret the map, all that is necessary is to examine a particular SNWS system and see how close it appears to a particular descriptor. Since the map is a two-dimensional representation of what is actually an n-dimensional space, the proximity of two points in the space is not always completely accurate or, at least, not sufficiently adequate for making final decisions. In general, however, the closer a SNWS system is to a descriptor on the map, the more people view that SNWS as being associated with that descriptor. For example, the SNWS system for submarines may be most closely associated with "jail" while the SNWS system for carriers may be mostly "feared."

The utility of this study can be best described by an analogy to marketing research. Marketing research has traditionally failed to consider and account for how the consumer fits within a broad array of findings and, thus, must make the tenuous assumption that self-descriptions are somehow related to the product or service. Careful and extensive research has shown that the distance of any item from the "me" in the map is strongly associated with the amount of time and energy people invest in that item. For example, political candidates closest to the "me" receive the most votes in elections, and products closest to the "me" are purchased more frequently.

In the application of the methodology to deterrence methodology, the analyst is trying to achieve the opposite, i.e., to move the "me" as far as possible from the SNWS system in question. This is accomplished by moving the descriptor rated farthest from the "me" closer to the specific SNWS system.

Essentially, this is a method of determining which concept, or set of concepts, out of the many combinations available, is most likely to

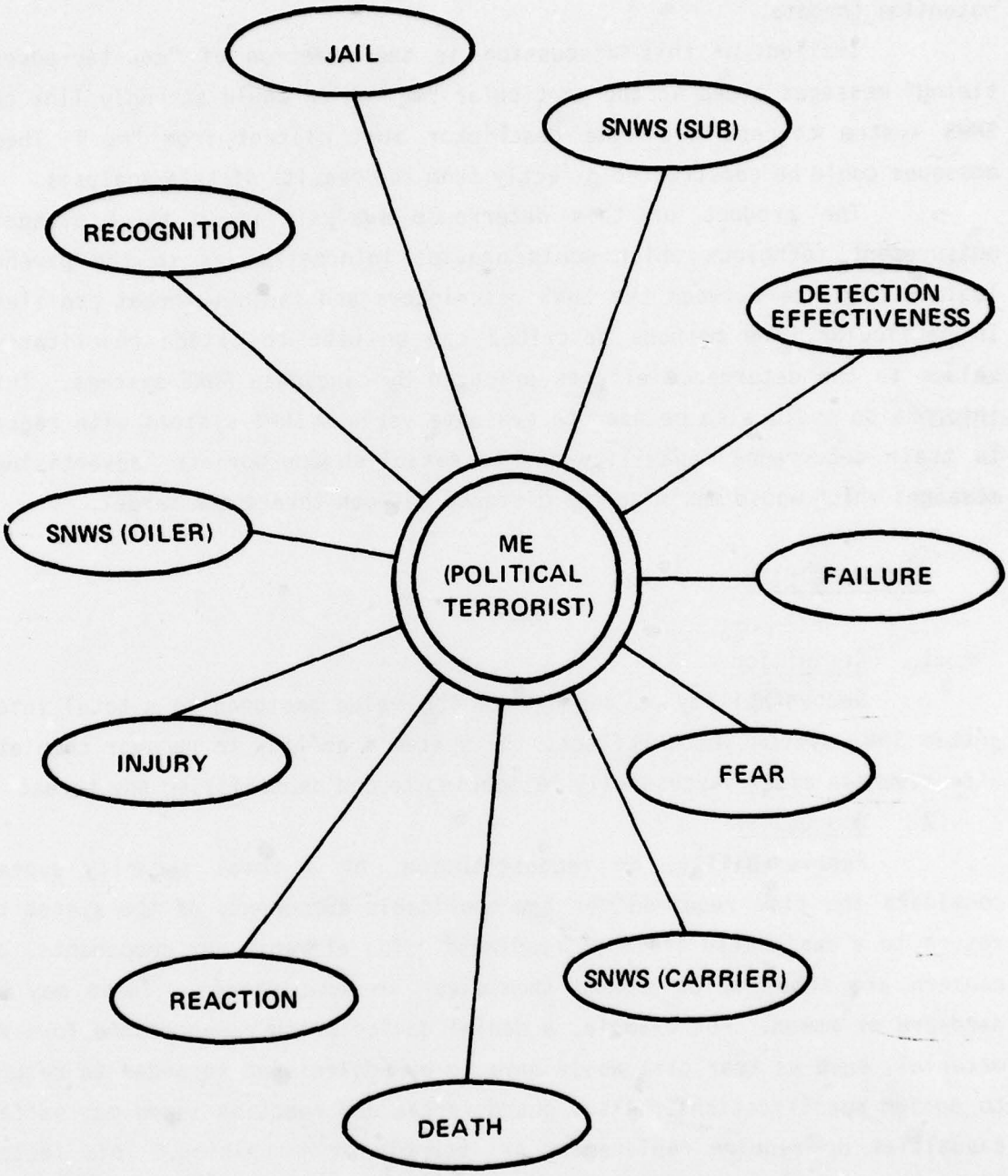


Figure 7-3. Deterrence Relationships

increase the psychological distance between a particular SNWS system and potential threats.

Implied in this discussion is the creation of "counter-advertising" messages aimed at the particular "me" which would strongly link the SNWS system concept with the descriptor most distant from "me." These messages could be constructed directly from the results of this analysis.

The product of this deterrence analysis would be a standard measurement technique which would provide information as to the psychological distance between the SNWS descriptors and various threat profiles. In particular, the methods described can be used to attach quantitative values to the deterrence effects produced by candidate SNWS systems. This information could also be used to evaluate various SNWS systems with regard to their deterrence capability and to establish appropriate "advertising" messages which would maximize the distance between threat and target.

C. RECOVERABILITY

1. Definition

Recoverability is defined as the value assigned to a total integrated SNWS system which reflects the system's ability to recover complete effectiveness after successfully responding to and neutralizing any threat.

2. Discussion

Recoverability, or reconstitution, of a total security system considers the time required for the applicable components of the system to return to a designated state of readiness. The elements, or components, of concern are those which expend themselves in some manner. These may be hardware or human. For example, a denial device which expends some form of material, such as tear gas, would have to be replenished in order to return to design specifications. Also, guard forces and reaction teams may suffer casualties or require replacement or resupply of ammunition. This factor of recoverability becomes important when postulating an intruder tactic of diversionary attack or attacks in waves intended to weaken the total security system. It is during this "recovery" period that the total SNWS system will not be as effective as it was designed to be.

3. Calculation

A Recovery Index (RI) may be calculated as a percent of tests in which the total security system fully recovers to design capability within a predetermined time limit. The mathematical expression would be:

$$RI = \frac{\text{\# RECOVERIES WITHIN TIME "T"}}{\text{\# TRIALS}}$$

D. APPLICATIONS

1. Purpose

This section presents ways in which deterrence and recoverability MOEs could be utilized by decision makers to assist in the selection of optimal SNWS system configurations.

2. Deterrence

Deterrence achieves its optimal utility when employed in the role of a "tie breaker." Given that all other MOEs are equal, a SNWS system that offers the greatest level of deterrence is of greater value, since the ideal system is one which would never have to be exercised to prove its worth.

For example, suppose it is the case that systems A and B both have the same costs, security indexes, and overall probability of security (P_{SEC}). However, system A has a deterrence rating of .9, while system B has a deterrence rating of .7 (the deterrence scale used here ranges from 0 to a maximim rating of 1.0). The obvious conclusion is that system A is more desirable than B.

3. Recoverability

The utility of the Recoverability Index can be evidenced in two areas. The first of these is in the role of a tie breaker, akin to that of deterrence. In this application, it could be used to evaluate SNWS systems against a multiple phased attack. The second use could be in concert with SNWS MOE, utilizing recoverability as a factor in the overall calculations. However, in order to preclude recoverability from biasing the methodology, the recoverability index (RI) should be damped by weighting based on the likelihood of such an attack.

CHAPTER 8
SUMMARY

A. GENERAL

The objective of this study effort was to develop a framework of measures of effectiveness (MOE) which could be used to objectively assess, evaluate and compare the performance and effectiveness of SNWs systems. Toward that end, a methodology has been developed which is independent of ship type, threat, operating mode or specific security system characteristics. The versatility of this methodology is further enhanced in that it can be employed at various aggregate levels, ranging from single ship/system component evaluation to fleet-wide assessments. The remainder of this chapter will serve to highlight the potential applications of the methodology and the conclusions and recommendations which have been drawn from the work performed in completion of this study effort.

B. APPLICATIONS

As presented in Chapters 5 and 6 of this report, there are three basic problem types to which the methodology developed in this study can be applied. These are:

- System Evaluation - Selection of an optimal security system from a range of candidate systems.
- System Requirements Definition - Pre-developmental establishment of security system/component performance requirements.
- System Design - Optimization of a mix of performance and cost constraints in order to select a system for multiple ship types.

One of the advantages inherent in the methodology is that it lends itself exceptionally well to computerization. This is particularly true for the applications of system evaluation and system design. Both of these could involve a lengthy and tedious exercise in numerical manipulation

if performed manually over a range of ship types, scenarios and threats. If, on the other hand, the algorithms presented in Chapters 5 and 6 were pre-stored in a computer, a virtually limitless variety of excursions would be available to the analyst. For example, the Friedman Two-Way Analysis Distribution - Free Test could be used in a sample exercise to determine if a set of candidate security systems were performing at the same level. Prior to conducting this test, a significant number of calculations are required in order to derive the figures of merit for each system on each ship type. These functions could be quite readily programmed on a computer, allowing the analyst to quickly perform the data reduction and analysis portions of the work. This would allow the analyst to spend more time looking at such excursions as the impact of zone weighting factors on test results or the imposition of minimum figure of merit criteria across all ship types in all scenarios.

Figures 8-1 through 8-3 illustrate how a representative program might be constructed. This program was written in BASIC for a desk top microcomputer equipped with a Cathode Ray Tube (CRT) display. The program was designed to be interactive, asking specific and direct questions to the user. Its simplicity facilitates quick learning by anyone possessing minimum familiarity with computer systems. As can be seen from the sample program printout, cost considerations could also be included in the system evaluation criteria.

The greatest utility of computer applications lies not with system evaluation, however, but with system design. Linear programming algorithms would greatly facilitate the formulation of security system performance requirements before hardware development. Given that there are over twenty types of ships which may carry nuclear weapons and that there is a wide diversity in possible threats and operating modes, a computer based program presents the only logical alternative for manipulating the quantity of data involved. The programming techniques are well known, and many commercial systems (CYBER-176 for example) currently offer software packages that include algorithms for the simplex method described in Chapter 6. It is envisioned that a computerized version of the SNWS MOE methodology

```
.
.
READY


DO YOU DESIRE INSTRUCTIONS; TYPE EITHER YES OR NO
?
YES


THIS PROGRAM CAN BE USED TO OBJECTIVELY ASSESS, EVALUATE, AND
COMPARE THE PERFORMANCE AND EFFECTIVENESS OF PHYSICAL SECURITY
SYSTEMS FOR SHIPBOARD NUCLEAR WEAPONS

THERE ARE SIX OPTIONS AVAILABLE ; THEY ARE:
OPTION          TITLE
  1          MOES VS. CLASS
  2
  3
  4
  5
  6          COST OPTIMIZATION

WHICH OPTION DO YOU DESIRE?  TYPE OPTION NUMBER  E.G. 3
?
 2

ONLY OPTION 1 IS CURRENTLY AVAILABLE

?
 1

OPTION 1  MOES BY CLASS COMPARISON
DO YOU DESIRE ALL CLASSES OF SHIPS?
?
NO
```

Figure 8-1. SNWS MOE Computerization

```
WHICH CLASSES DO YOU DESIRE?  THE FOLLOWING CLASSES ARE AVAILALE:
AS,AD,AO,AOE,AOR,AE,CG,CGN,CV,CVN,DD,DDG,FF,FFG,LHA,LPD,LPH,TAK
 1, 2, 3,  4,  5, 6, 7,  8, 9, 10,11, 12,13, 14, 15, 16, 17, 18
SSBN,SSN
  19, 20
INDICATE THE TOTAL NUMBER OF SHIP CLASSES TO BE CONSIDERED
?
 6

INDICATE CLASS/CLASSES TC BE CONSIDERED BY NUMBERED CODES SHOWN ABOVE
EACH SHIP CLASS MUST BE SEPARATED BY A COMMA, E.G. 1,4,19

?
 19  20  9  6  14  15

 ARE ZONAL WEIGHTS SATISFACTORY?
?
NO


INDICATE SHIP CLASS TO BE CHANGED BY NUMBERED CODE USED PREVIOUSLY
FOR EXAMPLE SSBN IS 19
 DO YOU NEED A LISTING OF THE SHIP CLASS CODES?
?
NO
?
 20


WHAT ARE THE NEW WEIGHTS FOR SHIP CLASS 20
EACH ZONAL WEIGHT MUST BE SEPARAED BY A COMMA;  E.G. .1,.1,.7,.1
PLEASE INSURE THAT THE SUM OF THE WEIGHTS EQUALS 1.0
?
 .05  .8  .1  .05


DO YOU DESIRE TO CHANGE ANY OTHER WEIGHTS?
?
NO
```

Figure 8-2. Interactive Computer Applications

OPTION 1 MOES VERSUS SHIP CLASS

LOCATION: IN PORT THREAT: SINGLE TERRORIST

	SSBN	SSN	CV	AE	FFG	LHA
MOE 1	.647	.715	.827	.612	.914	.317
MOE 2	.693	.409	.809	.715	.712	.466
MOE 3	.662	.589	.815	.216	.802	.299

THE OPTIMAL SOLUTION BASED ON MOE IS SYSTEM 1

Figure 8-3. Example Output Results

would lead to the eventual establishment of minimum performance criteria for detection, assessment, reaction and neutralization across all security zones, ship types and operating modes.

C. CONCLUSIONS

The SNWS MOE following conclusions can be drawn with regard to the product of this study effort.

1. Utility

The methodology is general enough to be applicable to all ship types, under any operational scenario, for any given threat, and for any type of SNWS system.

2. Practicality

The methodology is based on sound principles of security system operational requirements. The data required for calculation of performance measures is obtainable through standard techniques as outlined in Chapter 4. In particular the methodology is well-suited to accommodate data obtained from the SNWS Shipbcard Environmental Simulation Facility.

3. Flexibility

The methodology lends itself to a variety of applications. Evaluations can be performed for cases that range from the effectiveness of a detection system in a restricted scenario to the overall merit of a set of candidate systems for the entire fleet. In addition to the evaluation of existing systems, the methodology can be exercised to establish performance requirements for developmental systems, including design-to-cost considerations.

4. Ancillary Benefits

In addition to providing a tool for evaluating the effectiveness of SNWS systems, the methodology has provided a "roadmap" to the defintion of test data requirements for future evaluations of SNWS systems.

5. Implementation

The methodology is well-suited for incorporation on a simple, accessible microcomputer system. This step will ensure that the full

capability of the methodology is realized by providing the analyst with a wide variety of quick-response options for security system optimization and evaluation.

D. RECOMMENDATIONS

The following points are offered by way of recommendations for empirical evaluation of current or future SNWS systems, utilizing the methodology presented in the preceding chapters.

1. Automation

It is strongly encouraged that an interactive computer program be developed, along the lines of the example presented in Figure 8-1. Such a software system is highly desirable for evaluation of the large number of permutations and combinations of available security systems across the entire range of threats, scenarios, operating modes, ship platforms, and weapon types. With the algorithms for any desired test pre-stored in the data base, system planners can quickly analyze a wide variety of potential combinations, under any number of parameter setups, so as to maximize security while minimizing cost.

2. Human Factors

An analysis of human factors is recommended in order to accurately quantify the "man-machine" interface in any SNWS system. Human factors analysis techniques can be effectively and realistically applied to a quantification of the human role in the areas of detection, assessment, reaction and neutralization. Additionally, human behavior analysis techniques have been presented which could be employed to accurately determine the deterrence factors of candidate SNWS systems. This particular area has never been explored to any significant degree with regard to military security systems. A timely study effort would provide the necessary data base from which a future test bed could be employed to quantify the human contributions to overall physical security.

3. System Specification/Requirements

The versatility of the SNWS evaluation methodology presented in this study should be exploited to the fullest possible extent. Accordingly, it is recommended that the methodology be applied to the following types of design and developmental issues.

System performance requirements can be established for the functional areas of detection, assessment, reaction and neutralization. One method of employing the SNWS methodology to accomplish this would be to establish various combinations of performance measures which collectively result in a desired figure of merit for security. The optimum sets of functional performance measures could then be identified, subject to any number of selection criteria, including cost and unique shipboard requirements.

Some of the analytical methodologies cited in this report make use of minimum acceptable levels of functional performance which can be imposed as evaluation constraints. The SNWS methodology can be applied to evaluate these constraints, in order to develop realistic minimum levels, as part of the overall system design requirements.

Finally, maximum unit costs can be applied as constraints in the linear programming analysis. By utilizing the computer based analytic capability, the trade-offs between varying cost criteria, minimum security levels, zone weightings and the like can be analyzed. The result of such an analysis will facilitate the establishment of realistic, achievable, cost effective standards that must be met by manufacturers of security devices.

4. Test Plan

A final recommendation deals with the application of concepts presented as part of the SNWS MOE development process. Specifically, this study has provided a set of general guidelines for the types of data which are required for evaluation of SNWS systems. At present, none of these data are available. It is therefore recommended that the guidelines presented in this report for measurement of security system functional

performance be studied with emphasis on establishing specific requirements for SNWS evaluation data. The formulation of such requirements is an essential step to be completed during the planning phase of SNWS system tests.

APPENDIX A
GLOSSARY

TERM	DEFINITION
BISS	BASE INSTALLATION SECURITY SYSTEM
CCTV	CLOSED CIRCUIT TELEVISION
CRT	CATHODE RAY TUBE
DNA	DEFENSE NUCLEAR AGENCY
EDM	ENGINEERING DEVELOPMENT MODEL
FAR	FALSE ALARM RATE
FEDS	FORCED ENTRY DETERRENT SYSTEM
FIDS	FACILITY INTRUSION DETECTION SYSTEM
FMOE	FUNCTIONAL MEASURE OF EFFECTIVENESS
JSIIDS	JOINT SERVICE INTERIOR INTRUSION DETECTION SYSTEM
LLL TV	LOW LIGHT LEVEL TELEVISION
MOE	MEASURE OF EFFECTIVENESS
MTBF	MEAN TIME BETWEEN FAILURE
NPRDC	NAVAL PERSONNEL RESEARCH AND DEVELOPMENT CENTER
P_A	PROBABILITY OF ASSESSMENT
P_D	PROBABILITY OF DETECTION
P_N	PROBABILITY OF NEUTRALIZATION
P_R	PROBABILITY OF REACTION
P_{sec} (Z)	PROBABILITY OF SECURITY IN ZONE "Z"
P_{SEC}	PROBABILITY OF OVERALL SECURITY
RI	RECOVERABILITY INDEX
ROI	RETURN ON INVESTMENT
SESF	SHIPBOARD ENVIRONMENTAL SIMULATION FACILITY
SNWS	SHIPBOARD NUCLEAR WEAPON SECURITY
SNWSI	SHIPBOARD NUCLEAR WEAPON SECURITY INDEX
WIDS	WATERBORNE INTRUSION DETECTION SYSTEM